

METHOD, ARRANGEMENT AND APPARATUS FOR AUTHENTICATION THROUGH A COMMUNICATIONS NETWORK

Publication number: JP2002505458 (T)

Publication date: 2002-02-19

Inventor(s):

Applicant(s):

Classification:

- International: G06F1/00; G06F21/00; G06Q20/00; G07F7/08; H04L9/32; H04L29/06; H04Q7/38; G06F1/00; G06F21/00; G06Q20/00; G07F7/08; H04L9/32; H04L29/06; H04Q7/38; (IPC1-7: G07F7/08; H04L9/32; H04Q7/38)

- European: G06Q20/00K5; G06F21/00N5A2V3; G07F7/08; H04L29/06; H04L29/06S8; H04L29/06S18

Application number: JP20000533799T 19990205

Priority number(s): WO1999EP00763 19990205; FI19980000427 19980225

Also published as:

WO9944114 (A1)

US6430407 (B1)

IL138007 (A)

HK1036344 (A1)

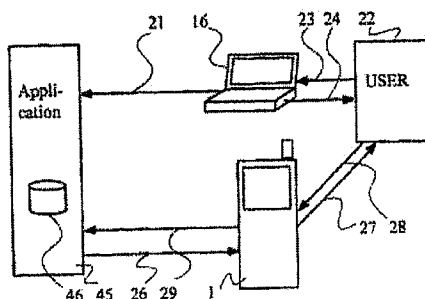
FI980427 (A)

more >>

Abstract not available for JP 2002505458 (T)

Abstract of corresponding document: WO 9944114 (A1)

A method, arrangement and apparatus for providing an authentication to an application provided through a communications network. A connection is established between the application and a user interface through said communications network so as to enable an access of a user to the application. An authentication is provided to said application by means of a mobile station communicating through a mobile communications network.



Data supplied from the *esp@cenet* database — Worldwide

(19)日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11)特許出願公表番号
特表2002-505458
(P2002-505458A)

(43)公表日 平成14年2月19日(2002.2.19)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 7 F 7/08		G 0 7 F 7/08	3 E 0 4 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 S 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 E 5 K 0 6 7 6 7 3 A

審査請求 未請求 予備審査請求 有 (全 59 頁)

(21)出願番号 特願2000-533799(P2000-533799)
(86)(22)出願日 平成11年2月5日(1999.2.5)
(85)翻訳文提出日 平成12年8月24日(2000.8.24)
(86)国際出願番号 PCT/EP99/00763
(87)国際公開番号 WO99/44114
(87)国際公開日 平成11年9月2日(1999.9.2)
(31)優先権主張番号 980427
(32)優先日 平成10年2月25日(1998.2.25)
(33)優先権主張国 フィンランド (F I)

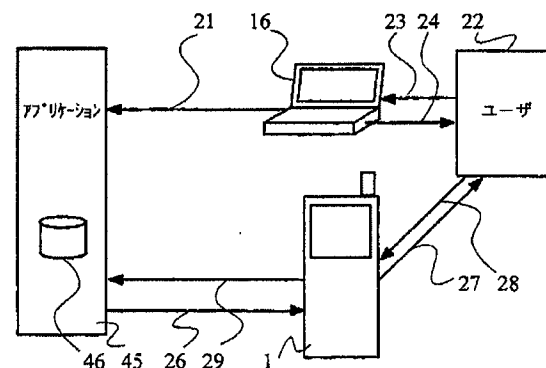
(71)出願人 テレフオンアクチーボラゲット エル エム エリクソン (パブル)
スウェーデン国エス - 126 25 ストックホルム (番地なし)
(72)発明者 ツルチアイネン、エサ
フィンランド国 エスポー、 カルタノンクヤ 8 エイチ
(74)代理人 弁理士 浅村 皓 (外3名)
Fターム(参考) 3E044 BA04 DA10 DE01
5J104 AA07 KA01 NA38 PA02
5K067 DD17

最終頁に続く

(54)【発明の名称】 認証のための方法、配列及び装置

(57)【要約】

通信網を通して提供されるアプリケーションに対して認証を与える方法、配列及び装置。アプリケーションに対するユーザのアクセスを可能にするように前記通信網を通してアプリケーションとユーザとの間に接続が確立される。移動通信網を通して通信する移動局により前記アプリケーションに対して認証が与えられる。



【特許請求の範囲】

【請求項 1】 アプリケーションのためにユーザを認証する方法であって、アプリケーションが第 1 の通信網を通してユーザに利用可能である方法において、

ユーザにアプリケーションをアクセスするのを可能にさせるように、前記第 1 の通信網を通してアプリケーションとユーザ・インターフェースとの間に接続を確立し、かつ

第 2 の通信網を通してアプリケーションと通信する移動局により前記アプリケーションに対してユーザを認証する方法。

【請求項 2】 認証のステップは、ユーザがユーザ・インターフェースによりアプリケーションをアクセスするときに、移動局を使用してユーザの識別を検証することを含む請求項 1 記載の方法。

【請求項 3】 認証のステップは、移動局を使用して、ユーザがユーザ・インターフェースを通してアプリケーションから前に要求したトランザクション又は処置に肯定応答することを含む請求項 1 記載の方法。

【請求項 4】 移動局はセルラ電話であり、かつ前記第 2 の通信網は、デジタル・セルラ網を含む前記請求項のうちのいずれかに記載の方法。

【請求項 5】 移動局の加入識別モジュール（SIM）の秘密を利用して認証ステップに関連したシグナリングを暗号化することを含む前記請求項のうちのいずれか一つに記載の方法。

【請求項 6】 移動局の加入識別モジュール（SIM）は、ユーザの識別を得るために使用される前記請求項のうちのいずれか一つに記載の方法。

【請求項 7】 ユーザ・インターフェースから SIM により識別された加入の保持者に対するアプリケーションへの接続のコストを請求するステップを含む請求項 6 記載の方法。

【請求項 8】 アプリケーションと移動局との間のシグナリングの少なくとも一部は、短メッセージの形式にあるシステム・テキスト・メッセージである前記請求項のうちのいずれか一つに記載の方法。

【請求項 9】 認証手順の 1 パラメータとして移動局のエリア位置情報を使用するステップを含む前記請求項のうちのいずれか一つに記載の方法。

【請求項 10】 通信網を通してユーザに利用可能なアプリケーションに認証を与える方法において、

アプリケーションに対するユーザのアクセスを可能にするように前記通信網を通してアプリケーションとユーザ・インターフェースとの間の接続を確立すること、及び

認証の暗号処理において移動局の加入識別モジュール（SIM）の秘密が利用されるように、移動局により前記アプリケーションに対して認証を与えることを含む方法。

【請求項 11】 通信網を通してアプリケーション・プロバイダにより提供されるアプリケーションに対して認証を与える配列において、

ユーザ・インターフェースと、

アプリケーションの使用を可能とする、前記通信網を介したアプリケーションとユーザ・インターフェースとの間の接続と、

アプリケーションの使用を認証する手段とを含み、前記認証する手段は、移動通信網を通して通信する移動局と、通信網の手段により実施されたアプリケーションと移動通信網との間のリンクとを含む配列。

【請求項 12】 移動局はセルラ電話であり、かつ移動通信網はデジタル通信網である請求項 11 記載の配列。

【請求項 13】 移動局へ及びからの認証シグナリングは、移動通信網の短メッセージ・システム（SMS）により与えられるテキスト・メッセージの形式にある請求項 11 又は 12 記載の配列。

【請求項 14】 移動局は、認証手順を制御するように配列された移動局の個人認証装置（MS PAD）と、秘密を含み、かつ MS PAD に作動的に接続された加入者識別モジュール（SIM）とを含み、SIM の秘密は、認証手順に利用されるように配列されている請求項 11 ～ 13 のうちのいずれかに記載の配列。

【請求項 15】 アプリケーションは、バンキング・サービス、電子ショッ

ピング・サービス、又は電子トランザクションに対して肯定応答を必要とする他のいくつかの商業的サービスであることを特徴とする請求項 11～14 のうちのいずれかに記載の配列。

【請求項 16】 通信網を通して提供されるアプリケーションに対して認証を与える移動局において、

アプリケーションは、通信網に接続されたユーザ・インターフェースによりアクセスされ、かつ

前記移動局は、ユーザ・インターフェースより通信のために異なる通信網を使用し、かつ移動局は、ユーザ・インターフェースによりアクセスされた前記アプリケーションの使用を認証するために使用される移動局。

【請求項 17】 認証手順を制御するように配列された統合移動局の個人認証装置（MS PAD）を含む請求項 16 記載の移動局。

【請求項 18】 局は、デジタル移動電話であり、かつ秘密を含む加入者識別モジュール（SIM）を含み、SIM の秘密は、認証手順に利用されるように配列されている請求項 16 又は 17 記載の移動局。

【請求項 19】 少なくとも 1 つの追加的な SIM を含む請求項 18 記載の移動局。

【請求項 20】 ユーザ・インターフェースと通信することが可能な赤外線又は無線トランシーバのようなユーザ・インターフェースと直接的にインターフェースをする手段を含む請求項 16 又は 19 記載の移動局。

【発明の詳細な説明】

【０００１】

（発明の属する技術分野）

本発明は、アプリケーションに対して認証を与える方法に関する。本発明は、更にアプリケーションに対して認証を与える配列、更に認証において使用される装置に関する。

【０００２】

（発明の背景）

認証のために必要となる種々の電子アプリケーションが存在する。認証は、例えば、ユーザが特定のアプリケーションをアクセスしているとき、及び／又はユーザが既にアプリケーションを使用しているときに、要求されることがあり、また、ユーザを検証する、又はアプリケーションにいくつかの更なる処理を許容するユーザからの肯定応答を受け取ることが必要となる。

【０００３】

認証が必要になると思われるアプリケーション例は、インターネット、イントラネット即ちローカル・エリア・ネットワーク（LAN）、通信網を通してアクセスされる支払い及び銀行サービス、リソース・アクセス、リモート・プログラミング、ソフトウェアの再プログラミング又は更新等のように、通信網を通して得られる種々の商業的なサービスを含む。通信網を通して得られるある種の無料サービスであっても認証を必要とすることがある。これらをアクセスしようとするユーザ（又サービスの使用中に認証をチェックする必要がある、若しくは使用中に何らかの承認する必要がある場合を除き、これらを既に使用しているユーザ）の少なくともある程度の認証を必要とするサービス若しくはアプリケーションの量は、過去数年の間に非常に増大した。更に、認証の必要性は、将来、一層増大することも予想される。

【０００４】

現在、通信の認証に関して既にいくつかの周知の解決法が存在する。通常、これらは、２つの通信コンピュータ装置間で種々の暗号化技術を使用する。基本的な認証シナリオによれば、前記２つのコンピュータ装置の暗号化機能に対してラ

ンダム・チャレンジ (random challenge) が与えられる。これらのコンピュータは共に、秘密 (secret) 即ち暗号鍵を有し、これは両コンピュータ内の暗号化機能にも与えられている。2つの暗号化機能の計算結果は、後で比較され、比較の結果が正となれば、その認証は有効であると見なされる。もし、比較が否定的な結果となれば、その認証テストは、失敗したと見なされる。

【0005】

更に、種々の既存の認証配列 (arrangement) が既に存在する。従来技術の下記例について、そのいくつかの欠点の簡単な説明をする。即ち、

【0006】

パスワード。現在、1つのパスワード、又はいくつかのパスワードの使用は、認証のための最も頻繁に使用されるアプローチとなっている。このパスワードは、ユーザ・インターフェースを通して、例えば通信網に接続されたコンピュータ端末を通してリモート・アプリケーションに与えられる。しかしながら、パスワードは網に対してアクセスを有する（及びパスワードを読み取るのに十分に熟練した）あらゆる者に曝されているので、この解決法は、網の脆弱性を考慮に入っていない。

【0007】

秘密。これは、例えばユーザ・インターフェースにより記憶されて使用される電子パスワード若しくは署名、又は暗号鍵として説明されてもよい。秘密が網に対して公開されていなくとも、結局は「悪行の手 (wrong hand)」に渡り、本来、秘密のユーザであることを意図していた者以外のあるグループにより使用される恐れがある。

【0008】

ユーザ・インターフェース内の認証ソフトウェア。これは、認証に対してより複雑なアプローチである。パスワードは、ユーザ・インターフェース内のプログラムに与えられ、このプログラムが要求されたアプリケーションに対する暗号アクセスを自動的に認証する。これは、以上の解決方法より安全な配列を提供するとしても、依然としてユーザ・インターフェースからパスワードを捕捉する可能

性が残っている。更に、実際のユーザに知らせることなく、ソフトウェアを変更することも可能である。

【0009】

スマート・カードとその関連のリーダー。スマート・カードは、暗号化された挑戦応答メッセージを通信することができるが、ユーザ自身からの認証を受け取るためのユーザ・インターフェースを内蔵していない。このようなインターフェースは、スマート・カード・リーダーに存在し得るが、このようなリーダーは、誤使用の可能性に対抗してうまく保護される必要があり、従って通常のユーザ（即ち、大多数のユーザ即ち公衆）は、通常、これらのリーダー・インターフェースに対して物理的なアクセスを有することができないが、これらは、スマート・カードを提供する組織を信用する必要がある。加えて、スマート・カード・リーダーは、互いに信用していない組織間では共有することができない。

【0010】

ユーザ・インターフェースを有するスマート・カード。これらは、既に存在するが、各安全プロセッサがそれ自身の安全ユーザ・インターフェースを有しなければならないので、高価になる。これらは、稀であり、その入出力機能は依然として極端に限定され、従って認証問題に対して経済的に適当な解決法であるとして保持されることはない。

【0011】

個別的な個人認証装置。このアプローチでは、ユーザがユーザ・インターフェースと個別的な認証装置との間の「通信手段」として使用される。従って、ユーザ・インターフェースは、ユーザが携帯認証装置（ポケット電卓のような装置）にタイプ入力する挑戦を受ける。認証装置は、応答として例えばある数を与えてもよく、従ってユーザは、この数をユーザ・インターフェースにタイプする。ここで、問題は、個別的な装置を購入し、携帯して使用する必要性に関係する。更に、いくつかの例では、通常、長く複雑なキャラクタ・ストリングを不正確にタイプ入力する可能性も存在する。

【0012】

以上は、既に、この認証システムを実施するときに係わり得るいくつかのグル

ープについて述べている。以下、これらを更に詳細に説明する。

【0013】

ユーザは、通常、種々のアプリケーション又はサービスを使用する人間である。ユーザは、彼又は彼女のみが知っているパスワード（即ち秘密）（public key method：公衆鍵方法）により、又はユーザとアプリケーションとの間で共有される秘密（secret key method：秘密鍵方法）により、識別可能とされる。

【0014】

このアプリケーションは、ユーザの認証を保証したいグループである。更に、サーバと呼ばれるいくつかの場合においても、このアプリケーションを呼び出すことができる。アプリケーションの観点から、認証質問を4つの異なるカテゴリ（質問）に分けることができる。（1）は、その時点で他端にいるユーザか？（いわゆる対等者存在の認証（peer entity authentication））、（2）は、同一ユーザから更なるメッセージを受信しているのか？（メッセージ・ストリームの保全）、（3）あるユーザから発生している特定のメッセージか？（データ発生源認証）、及び（4）第3のグループであっても一定のユーザから発生していると思われるようなメッセージか？（非拒否）。

【0015】

ユーザ・インターフェースは、ユーザにアプリケーション又はサーバをアクセスできるようにする装置又は配列である。大抵の場合、これを端末と呼ぶことができ、コンピュータ（例えば、パーソナル・コンピュータ、PC）、ワークステーション、電話端末、移動電話又は無線又はページャのような移動局、現金自動預払い機、及び／又はバンキング・マシン等のような装置からなるものでよい。ユーザ・インターフェースは、入出力機能を提供し、またアプリケーションの一部を提供することも可能である。

【0016】

個人認証装置（PAD）は、ユーザが自ら搬送するハードウェアのうちの1つである。PADは、いくつかの基本的な入力／出力機能、更にはいくつかの処理機能も有することができる。以上で述べたスマート・カード及び別個的な認証装

置は、PADと見なされてもよい。大抵の場合に、ユーザは、そのPADを（殆ど）常時、携帯して、従って連続的に規制をしているので、ユーザは、そのPADに依存することができる。全ての可能パスワード即ち秘密は、これらを簡単な方法で明かせないようにハードウェアそのものに隠される。装置そのものは、ユーザとセキュリティ・プロセッサとの間の通信パスが危険にさらされないように、容易に変更できない。加えて、PADは、通常、記憶された状態の最小量を有し、プログラムそのものは容易に変更できない。

【0017】

（発明の概要）

認証に関して、以上で述べた従来技術の解決方法が既に存在しているといえども、認証のエリア内で、以上で既に言及したものに加えて、まだいくつかの欠点が存在する。

【0018】

アプリケーションに対するアクセスが絶対的に安全、又は可能な限り安全にされている場合に、アプリケーションは、そのアーキテクチャーが容易に極端に複雑化することになり、また、アクセスして使用するために複雑化し、かつより時間が掛かるものとなる。セキュリティ・レベルを増加させれば、所要ハードウェア及びソフトウェアの量を増加させ、これがその保守及び更新のための必要性を増加させるに至り、従って、認証の総合コストは、高くなる恐れがある。複雑化及びコストは、セキュリティのレベルを下げることにより低減可能だが、これは通信が、十分でないセキュリティ・レベルに至ると予想される。加えて、技術的な進歩は、ハッカー達が最も複雑化したセキュリティ配列さえも解き明かすのを可能にさせるので、通信網において「絶対安全」条件さえも存在しないと信じる。

【0019】

人間の問題は、パスワード即ち秘密が極めて複雑かつ／又は長すぎる、又は沢山あり過ぎることになり得ることである。従って、ユーザはこれらを記憶するのが困難なことに気付くことになり得る。典型的には、秘密鍵方法において安全と見なされている秘密は、128ビットであり、また公衆鍵方法では1024ビット

トである。殆どの者は、この種の鍵を思い出すということが不可能である。

【0020】

加えて、ユーザは、外部装置なしに認証に必要とされる計算を実行することができない。以上で説明したように、基本的な認証は、しばしば挑戦及び応答の方法により行われる。これは、ユーザ（即ち、人間）が彼の秘密により、何らかのものを暗号化することが必要となる。これは、実際において続けていられない。

【0021】

今日の解決方法は、以上で説明したように、開放された通信網で伝送中にパスワード又は秘密を捕捉する可能性に加えて、いずれもユーザ・インターフェースの脆弱性に対して十分な注意を払っていない。端末装置は、複雑極まりない技術及びソフトウェアを開発したので、多くのユーザは、端末を十分に制御すること、又はその動作を理解することはもはや不可能である。加えて、多くのユーザが同一の端末装置（例えば、共通使用のPCである。）を共有すること、及び／又は外部の保持要員が本質的に非公開機関のコンピュータに対するアクセスを有することがしばしば発生する。

【0022】

コンピュータ端末は、そのメモリ手段に、記憶された状態及びプログラムを備えており、これらは変更可能である。最近のコンピュータでは、ユーザがソフトウェアの変更気付かないように、また物理的に装置そのものにアクセスすることなく、通信パスを通すように、そのソフトウェアを変更することさえも可能である。リスクの1例を挙げると、ユーザが例えばある銀行に送出するデータを変更するように、コンピュータがある日に全ての銀行間の振替をユーザ（利用者）により指定されていたもの以外の他の預金口座に変更するように、コンピュータ端末内のプログラムを変更することも可能である。通告のないこの変更又は再プログラミングは、通常の個人的なユーザに対して使用されたとき、特に会社又は公的な機関のような組織に対して使用されたときは、深刻かつ莫大な損害を発生させる恐れがある。これは、全て通常の端末装置及び通信パスが信頼されないことを意味する。

【0023】

従って、本発明の目的は、従来技術の解決方法の欠点を克服すると共に、認証に対して新しい形式の解決方法を提供することである。

【0024】

更に、本発明の目的は、アプリケーションをアクセスしたいユーザを従来技術において可能であったものより安全な方法により認証することができる方法及び配列 (arrangement) を提供することである。その目的は、認証の必要性が既にアクセスしたアプリケーションの使用中に発生したときに、認証を与えることである。

【0025】

本発明の目的は、認証において移動局を利用することができる方法及び配列を提供することである。

【0026】

本発明の追加的な目的は、認証において移動局の識別モジュールを利用することができる解決方法を提供することである。

【0027】

本発明の他の目的及び効果は、添付図面に関連させた明細書の下記部分により達成される。

【0028】

これらの目的は、通信網を通して供給されるアプリケーションに認証を与える新しい方法により得られる。本発明によれば、通信網を通して提供されるアプリケーションに対してユーザのアクセスを可能にさせるように、アプリケーションと前記通信網を通るユーザ・インターフェースとの間の接続が確立され、同時に移動通信網を通して通信する移動局により前記アプリケーションに対する認証が与えられる。

【0029】

更なる一実施例によれば、認証方法は、通信網を通して提供されるアプリケーションに対してユーザがアクセスできるように、アプリケーションと通信網を通るユーザ・インターフェースとの間に接続を確立するステップを含む。前記アプリケーションに対する認証は、認証の暗号処理において移動局の加入者識別モジ

ジュール (Subscription Identification Module: SIM) の秘密を利用するように、移動局により提供される。

【0030】

本発明は、更に、通信網を通してアプリケーション・プロバイダにより提供されるアプリケーションに対する認証を与える配列を含む。この配列は、アプリケーションを使用できるように、アプリケーションと前記通信網を通るユーザ・インターフェースとの間の接続とを含む。この配列は、更に、アプリケーションの使用を認証する手段を含み、前記認証するための手段は、移動通信網を通して通信する移動局と、通信網により実施されるアプリケーションと移動通信網との間のリンクとを含む。

【0031】

他の実施例によれば、本発明は、通信網を通して提供されるアプリケーションに対して認証を与える移動局を備える。この実施例において、前記移動局がユーザ・インターフェース以外の、通信のための異なる通信網を使用している間に、アプリケーションは、通信網に接続されたユーザ・インターフェースによりアクセスされる。前記移動局は、ユーザ・インターフェースによりアクセスされる前記アプリケーションの使用を認証するために使用される。

【0032】

この解決方法は、認証に対して信頼性のある新しい方法を導入しているので、本発明によりいくつかの効果が得られる。本発明の認証方法及び配列は、余分な代替又は追加的な装置なしに、既存の通信網に容易に実施できる。この配列は、実際において、ある種の認証を必要とする通信システムを通して提供される任意のアプリケーションと関連して、異なる種々のアプリケーションとの接続に使用されてもよい。

【0033】

ユーザは、別個の認証装置 (PAD) 又は異なる多くの認証装置を搬送することから開放される。更に、ユーザは、通常、移動局が常にユーザと共にあり、かつユーザがこれらの移動局をよく管理する傾向があるので、本発明による個人認証装置 (Personal authentication device: P

A D)を信頼することができる。加えて、例えば窃盗の移動局の場合は、移動電話加入者及び／又はそのS I Mをオペレータにより容易に取り消すことができる。移動局の全ての秘密は、これらを容易に明かさないように、そのハードウェアに首尾よく隠されている。加えて、移動局の装置自体は、ユーザとセキュリティ・プロセッサとの間の通信パスを危険にするように容易に変更され得ない。

【0034】

システムは、最小量の記憶状態を含み、かつプログラムは容易に変更され得ない。移動局の既存S I M、より具体的に、その秘密は、必要とする暗号化手続に利用されてもよい。従って、S I Mは、新しい目的用のセキュリティ・カードとして利用されてもよく、また、虚偽の疑いがあれば、S I Mの使用を制御する既存のパーティ、即ち直ちにS I Mを取り消すことができる移動電話網のオペレータが存在する。

【0035】

以下、添付図面を参照して本発明及び他の目的、並びにその効果を添付図面を参照して複数例により説明するが、種々の図面を通して同一参照番号は、同一の機能を表している。本発明の以下の説明は、本発明をその接続により提供された特定形式に限定されず、それよりも本発明は、付記する請求の範囲の精神及び範囲に含まれる全ての変形、類似性及び代替を包含することを理解すべきである。

【0036】

(発明の詳細な説明)

図1は本発明を実施するときに使用することができる一つの網配列の概要図である。図1の配列は、20により表すブロックとして概率的に示されている公衆交換電話網(Public Switched Telephone Network: PSTN)を含む。例示したPSTNは、固定回線電話網(又はプレーン旧電話サービス(Plain Old Telephone Service: POTS))であって、これは、アプリケーションをアクセスできるようにユーザ・インターフェース16を可能にする通信網を形成する。この実施例によれば、ユーザ(図示なし)は、インターネット接続を通して得られるWWWサーバ45のうちの1つにより所望のサービスにアクセスするように、ユーザ・インタ

ーフェースとして、PSTNに接続されたユーザ・インターフェース16を使用することができる。開示された端末16は、パーソナル・コンピュータ（PC）であるが、しかし更にワークステーションのように他の形式のユーザ・インターフェース、現金自動預払い機等を使用することもできる。

【0037】

更に、公衆地上移動電話網（Public Land Mobile Network：PLMN）を開示する。これは、例えば、セルラ電話網又は同様の移動通信システムであってもよい。更に、移動局MS1及びMS+PC2も開示する。MS+PC2は、統合された移動電話及び携帯コンピュータとして定義されてもよい。これらは共に、エア・インターフェース3を通して、PLMNのいくつかの基地局（BS）4のうちの一つを通るPLMNと通信することができる。

【0038】

PLMNの1形式は、ETSI（European Telecommunications Standard Institute：欧州電気通信標準委員会）によるGSM提唱においてよく規定されているデジタルGSM網（Global System for Mobile communication：GSM：移動体通信グローバル・システム）であり、その網構成自体は、推奨GSM01.02若しくはGSM03.02、又はその改訂版に詳細に記載されている。本発明は、主としてGSMの技術用語を使用して例示的なセルラ電話網に関連して説明されていることに注意すべきであり、当該技術分野において通常に習熟する者は、この発明を任意の移動システムに実施できることを理解すべきである。更に、明確にするために、例示的なシステムの動作を説明する目的のために、必要と考えられる移動電話網構造の複数部分のみが示されていることに注意すべきである。習熟する者は、電話網が通常、説明したものより必要とする他の装置を含めてもよいこと、PLMN又はPSTNの開示したいいくつかの要素が省略又は他のなんらかの形式の複数要素により置換されてもよいこと、及び多数の移動電話網及び通常の固定地上回線網が互いに協同し、かつ交換してもよいことに確かに気付く。習熟する者は、インターネットに対する接続が如何なるPSTN、又はユーザ・インターフェース16とインターネット43との間における

同様の網構成のない、直接接続であってもよい。しかしながら、これらの代替は、当該技術分野において通常に習熟する者に知られているので、更に詳細に示し、また説明もしていない。

【0039】

公衆地上移動電話網（PLMN）に基づくGSMは、通常、いくつかの移動サービス交換局（mobile service switching center：MSC）10を含む。続いて、これらはそれぞれが複数の基地局サブシステム（BSS）6（明確にするために1MSC及びBSSのみが示されている。）に接続される。基地局サブシステム6は、通常、基地局コントローラBSC及び必要とするインターフェース装置を含み、かつ複数の基地局（BS）8に接続され、それぞれはセルと呼ばれるある地理的なエリアを管理する（セルについては、図7を参照）。

【0040】

図1の移動サービス交換局10は、更に、交換12及び回線12を通じて公衆交換電話網（PSTN）20に接続又はリンクされる。更に、MSC10は、例えば、（番号43により指示された）インターネットであるグローバル通信網にも接続される。MSCは、総合ディジタル通信網（ISDN）又は適当な他の形式の通信網に接続されてもよい。異なる電気通信網システムの異なる構成要素間で必要とするリンクは、それ自身が当該技術分野において周知である。

【0041】

PLMNは、更にデータ・ベース、MSCに接続されたいわゆるホーム位置レジスタ（home location register：HLR）9を含む。移動電話網の加入者であるこれらの移動端末1及び2は、HLR10に登録される。各ローカル移動電話交換局10は、更に、訪問者位置レジスタ（visitor location register：VLR）8と呼ばれる各ローカル・データ・ベースを含み、これには、任意の与えられた時点で、移動電話がそのローカル移動電話サービス交換局MSCにより処理されるセルのうちの1つのエリア内に位置した全ての移動局1及び2が登録される。

【0042】

移動局は、通常、これらの移動局のそれぞれ内に搭載された、そうでなければこれに物理的に接続されたSIM (Subscriber Identification Module: 加入者識別モジュール) により識別される。SIMは、情報及び秘密に関係した種々のユーザ (加入者) を含むモジュールである。これは、更に、無線通信の暗号化に関係する情報を含めてもよい。SIMは、移動局に固定的に又は削除可能にアセンブリされてもよい。本発明におけるHLR及び/又はVLRレジスタと共に、SIMの利用を以下、この明細書において更に詳細に説明する。

【0043】

以上で説明したように、ユーザは、固定若しくは移動電話網を通して、又は直接接続を通してインターネット43に接続されてもよい。しかしながら、例えばGPRS (General Packet Radio System: 汎用パケット無線システム) に関係するときに、接続間にはいくつかの相違が存在し得るが、しかしインターネット網のサービスは、PSTN及びPLMNシステムの両ユーザに利用可能である。この例では、PSTN20と共に移動通信交換局 (MSC) 10がアクセス・ノード (AN) 14及び40により、マルチプロトコル・インターネット43に対してアクセスが提供される。1通信網当たり1ANのみであっても、実際において、ANの数が本質的に更に大きくされてもよく、更にAN数が連続的に増加していることが理解される。一解決方法によれば、信号をデータ・パケットに変換することができる特殊なインターネット・アクセス・サーバIASがインターネットに向けてのANとして使用される。

【0044】

インターネット43のユーザは、ユーザ端末1、2又は16からインターネットに対して通信接続を行うインターネット・サービス・プロバイダ (Internet Service Provider: ISP) 42との接続を行った。ユーザがインターネット接続をしたいときは、ユーザがその所望のアドレス (いわゆるインターネット・プロトコル・アドレス) にユーザの端末16に接続するように、インターネット・サービス・プロバイダ (ISP) 42に対して呼出しをする。呼の接続は、PSTN20により確立されて、少なくともローカル交換

18を通過して、多分、トランク回線（図示なし）を通過して接続又は相互接続される一又はいくつかのトランジット交換を通過する。図1は、両通信網がインターネットに向かって通信する唯一のISPのみを開示しているが、通信は異なるISPを通過するように配列されてもよいことを理解すべきである。

【0045】

図1は、更に、異なるサービスを提供するサーバ・データベースx、y及びzを含むWWWサーバ45（World Wide Web server：ワールド・ワイド・ウェブサーバ）を開示している。これはISPからルータ44を通過し、インターネット43を通過する前記サーバ45への接続を開示している。サーバは、認証を必要とするバンキングサービス、電子ショッピング・サービス等のように、任意の通信網を通過して得られる任意のサービスであってもよいことを理解すべきである。

【0046】

移動局1（又は2）は、ユーザがユーザ・インターフェース16を介し、PS TN20を通過してWWWサーバ45により提供されるサービスxにアクセスするとき、又は既にアクセスしたときに、個人認証装置（personal authentication device：PAD）として使用される。移動局1は、チャンネルが実際のユーザ・インターフェース16により使用されるよりも、別個の通信パス即ちチャンネルを通過してサービスxと通信する。移動局は、通常、ユーザがこれを常時、保持しているので、信頼できるとされる。移動局及び通常のPADに対する人間工学及び機能的な必要条件は、本質的に同一であり、MSはPADに適したユーザ・インターフェースを有する。最近のMSは、認証目的に適したセキュリティ・プロセッサ・インターフェースさえも有する。

【0047】

移動局による認証を達成するいくつかの代替があり、ここで、その複数例を以下で更に詳細に説明する。

【0048】

ここで、図2及び4を参照する。図2は認証のための1配列、また図4は基本的な一実施例による動作のフロー・チャートを概念的に開示している。ユーザ2

2は、通信網（図2における矢印21、図4におけるステップ102及び104）により確立された接続を通るバンキング・サービスのよう、所望のアプリケーション45をアクセスする要求をユーザ端末16により送出する。アプリケーション45は、データ・ベース46を含んでもよく、又は図1のMSC10のHLR9のように、別個のデータ・ベースに接続され、これによりアプリケーションは、必要とするユーザ情報を抽出できるようにされる。この情報に基づいて、アプリケーションは、認証目的のためにユーザ22の移動局1に対する接続を確立する（矢印26、ステップ106）。この段階で、ユーザは、移動局1を使用して、アクセスが許可され、かつサーバの実際の使用が開始できることを表す確認信号29（即ち、肯定応答）を返送することにより、ユーザ・インターフェース16により作成した接続21を受け付けることができる（ステップ108及び112）。例えば、アプリケーションがMS1に到達できないことに基づき、認証失敗の場合は、全ての接続が閉鎖される（ステップ110）。代替として、ユーザが直ちに又はある時間後にアクセスを再試行するのが許可されても、又はユーザが失敗した認証のためにユーザ・インターフェース16によりいくつかの追加的な措置を取るように指令されてもよい。

【0049】

認証又は肯定応答機能を実行する方法は、PLMNの短メッセージ・システム（SMS）の短メッセージを使用することである。GSMシステムにおいて、移動局へ及びからの短メッセージを送出するために、図1に7により表されているSMS MSC（SMS Message Service Center：SMSメッセージ・サービス・センタ）が設けられる。以上で説明し、かつ言及した仕様により定義されたように、同一の網構成要素を使用して、サービス・センタ7は、移動電話加入者にメッセージを送出する。SMSメッセージ・シグナリングは、通常、例えば受信機識別、送出情報、タイム・スタンプ等を含む。

【0050】

図3は、移動局MS1がSMSメッセージを受信した一解決方法を開示している。このための方法ステップは、図5のフロー・チャートにより示されている。この実施例によれば、ユーザは、ユーザ・インターフェース16を通してバンキ

ング・サービスをアクセスした後に、200FIMの和がアカウントNo. 1234-4567からアカウント4321-7654に振替されるべきことを要求した（ステップ204）。従って、アプリケーションは、適当なデータ・ベースからユーザ関連の認証データを取り出し（ステップ206）、かつ移動局1にテキスト・メッセージを送出する（ステップ208）。MS1は、図示のようにテキストを表示し、ユーザに、「イエス」又は「ノー」キーをそれぞれ押すことによりトランザクションを肯定又は否定するように、質問をする（ステップ210）。次いで、応答がアプリケーションに返送されて、「イエス」の場合は、トランザクションが進み（ステップ214）、「ノー」の場合は、他のいくつかの処置を取る。

【0051】

更に、図2の矢印27と28がMS1及びユーザ2が通信する段階を示しており、MS1のディスプレイ31で見ることにより受信される情報が矢印27により示され、ユーザによりMS1に与えられる応答が矢印28により示されている。説明したように、ユーザは、MSのY又はNキー32を押すことにより、適正な選択を選択できる。従って、ユーザが受け取った即ちトランザクションに「署名」した場合は、バンキング・サービスが進む。ユーザがトランザクションを確認しない即ち「ノー」キーを押した場合は、アプリケーションは、ユーザ・インターフェースに訂正、取り消し、新しい宛先アカウント等を入力するように要求することができる（ステップ216、218）。

【0052】

ある期間内でアプリケーションが応答を受信しない、又は応答がいずれにしろ誤っている場合は、アプリケーションは、確認、又は全ての接続を閉鎖するための第2の要求を送出することができる。

【0053】

ユーザは、次のいくつかのトランザクション、更には一旦アプリケーションをアクセスした後に他のいくつかのバンキング・サービスをも処理することができる。ステップ216において、ユーザが最終的にユーザ・インターフェース16に対して、ユーザが継続したくないことを応答するときは、接続が閉鎖される（

ステップ220)。

【0054】

本発明の一実施例によれば、本発明の認証配列を実施する際に、図1のPLMNのHLR、更にはVLRに含まれる情報を利用することができる。これは、移動電話加入者のそれぞれが、図1のHLR9内に、位置情報(VLR番号)、基本電気通信サービス加入者情報、サービス規制及び補助サービス等と共に、既に述べたSIM(加入者識別モジュール)、IMSI(International Mobile Subscriber Identity:国際移動電話加入者識別)、及びMSISDN(Mobile Subscriber ISDN Number:移動電話加入者ISDN番号)に関連した情報を含むということにより、可能にされる。

【0055】

従って、更に、MS1内に挿入されたSIM(Subscriber Identification Module:加入者識別モジュール)カード34を開示する図3を見ることができる。電話会社は、通常、ユーザの支払い及び位置を制御するためにSIMを使用する。従って、SIMカード34は、使用状態にして、電話呼出をする前に、MS1に接続される必要がある。図3のMS1は、更にMS PADコントローラ35(Mobile Station Personal Authentication Device controller:移動局個人認証装置コントローラ)を含む。本発明では、これらにより、SIM34は、ユーザを識別し、かつ/又は一秘密又はいくつかの秘密を含む手段として使用されてもよく、またMS PADコントローラ35は、認証処理を制御するために使用される。コントローラ35は、認証手順の一般的な制御に加えて、例えば種々の暗号化処理に関連する全ての計算を行うように配列されてもよい。認証手順において、MS PADコントローラ35により制御されるSIM34を利用することができる配列は、種々である。

【0056】

SMSサービスを利用する前述の配列の代わりに、トランザクションは、更に、例えば電子的なトランザクションにより支払われるバンキング・サービス又は

他の商業的なサービスのようなアプリケーションがMS PAD35に対するトランザクションの詳細をMS PAD35に移動電話網を通るデータ信号として送出するように、肯定応答されてもよい。信号の正しさは、予め定めたアルゴリズムに従い、かつSIM34の秘密を利用して、MS PAD35により計算されたチェックサムにより保証されてもよい。即ち、チェックサムは、ユーザ端末16により表示されたサムと一致する必要がある。ユーザがトランザクションを受け入れると、ユーザは、これに肯定応答をし、かつ（例えば、公衆キー暗号化及び無拒否の使用を必要とするときに）ユーザの秘密を使用する、又はアプリケーションと共用される秘密を使用することにより、アプリケーションからのメッセージ信号26に「署名」するように、MS PAD35に対して許可を与える。その後、アプリケーションは、ユーザ・インターフェースによる要求に従って進行する。一実施例によれば、更に、SIM34の秘密又は複数の秘密は、メッセージの暗号化、及び／又はアプリケーションとMSとの間のシグナリングに使用されてもよい。

【0057】

図6は図2に対する他の実施例を開示する。この実施例において、ユーザ・インターフェース16は、それ自体が公知の方法によりPSTN20に接続された通常の電話端末の形式にある。PSTNは、更にこの実施例においてアプリケーションを形成するインテリジェント・ネットワーク・サービス（*intelligent network service*:IN）60に接続される。移動局1は、図3に関連して以上で説明したPADコントローラ35及びSIM34を含む。一実施例によれば、与えられたサービスに対するサービス識別子と個人秘密とを含むMS PAD対がPADコントローラ内に記憶される。これらの対は、例えば以下の方法で使用される。

【0058】

ユーザは、サービスに対する電話呼を確立することにより、前記INにサービスをアクセスする（矢印21）。アプリケーションは、音声メッセージとして与えられた番号により、又は前記電話端末上の可能ディスプレイにより、ユーザに挑戦する（矢印61）。この挑戦において、ユーザは、キーパッドによりMSに

対して、特定の番号と一緒にキー入力し（矢印28）、その後、PADコントローラは、更なる番号のつながりを受信するように、好ましいアルゴリズムに従って必要な計算達成する。この計算において、特定のユーザのためにSIMに記憶した秘密は、アルゴリズムの一部を形成することができる。この秘密は、アプリケーション特定秘密又はPLMNの秘密であり得る。次いで、計算の結果は、ユーザ・インターフェース16に供給され（矢印62）、PSTN20を通る質問によりINサービスに送信される。これが期待した値と一致した場合は、INサービス60は、ユーザが固定回線端末16によりこれを使用するのを許可する。

【0059】

以上で述べた実施例は、例えば通常的な任意のPOTS回線電話を通して得られる電話呼出又はサービスを支払うときに、使用されてもよい。例えば、これは、任意の電話端末による呼が移動電話加入者から（即ち、特定のSIMカードの所有者から）課金される配列を可能にする。移動電話加入者は、例えば移動電話により発生した呼が通常のPOTS電話による呼よりも高価となる場合、又はMS1がユーザが正しい無線接続を確保できる移動電話網のエリア内に存在しないときに、このサービスが有用なことが解る。

【0060】

追加的な一実施例（図示なし）によれば、移動局1及びユーザ・インターフェース16は、無線接続、赤外線接続、又は必要なカップリングによる固定管路接続のような適当な運用上の接続により、相互に直接通信することができる。これは、MS1とユーザ・インターフェース16との間の「リンク」として動作しているときに、ユーザが犯すかも知れないタイプ誤りの危険性を軽減する。

【0061】

一つの代替によれば、移動局は、1以上のSIMカード34を受け入れるように配列される。これにより、異なる認証目的に1移動局を使用することができる。例えば、ユーザは、異なる3つのSIM、即ち、ユーザの作業に必要とされる認証用に一つ、個人用に一つ、及び更なる必要性のため、例えば「協会の議長」用に一つを備えることができる。これらのSIMはそれぞれ、それ自身の電話番号、アラーム・トーン等を有することができる。

【0062】

更なる代替によれば、MS 1はPLMNを通してアプリケーションと通信し、かつこの通信に必要とするメッセージ及び／又はシグナリングがSIMの秘密又は複数の秘密を使用して暗号化される。これは、SIMの秘密が固有なときに、唯一の通信網、即ちPLMNのみを使用して安全通信を可能にさせ、また第3のグループがシグナリングに含まれている情報を得ること、又はシグナリングに割り込むことが不可能となる。

【0063】

ここで、図1及び7を参照して本発明の更なる実施例を説明する。図7は複数の連続的な無線サービス・エリア、即ち複数のセルに分割された任意の地理的領域の概要セル・マップを開示する。図7のシステムは、10セル（C1～C10）のみを含むように示されているが、セルの数は、実際にはもっと多数となり得る。1基地局がセルのそれぞれに関連され、かつその内部に配置される共に、これらの基地局がそれぞれBS1～BS10と表されている。これらの基地局は、基地局サブシステム（図1のBSS6）に接続されている。更に、1セルは、1又はいくつかの基地局をカバーしてもよい。これらのセルは、4グループA～Dにグループ分けされ、各グループは、対応するマーキングによりマークされているように、1以上のセルを含むことができる。

【0064】

各グループは、異なる4セル・カテゴリA～Bを設けるように、システムによって1ユニット即ち1エリアと見なされる。その目的は、これらのセルを異なる複数の認証カテゴリ、即ち複数のクラスに分割できることを示すことにある。その背景の概念は、ユーザがある予め定めたセル・エリア内に位置していない場合に、認証データ・ベース内の認証データは、ユーザにアプリケーションをアクセスするのを許可しない規制を含めてもよいということである。例えば、会社が認証に関して被雇用者のMSを使用するときは、認証の可能性を規制してその会社の事務所の近傍にあるセル内（例えば、エリアA内）のみで許容するように、エリアを制限することができる。

【0065】

以上は、図1内の8により表された訪問者位置レジスタVLRにより、容易に実施可能である。MSCのエリア内をローミングしている複数の移動局（MS）1又は2は、そのエリアに対して責任を持つVLR8により管理される。VLR8は、MS1又は2が位置エリアに出現するときは、VLRは更新手順を開始する。更に、VLR8は、例えばMSが、IMSI、MSISDN、及び例えばGSM09.02仕様に従って登録される位置エリアを含むデータ・ベースも有する。いわゆるセル・グローバル識別は、更に、セル識別を含み、かつMS1とMSC10との間のメッセージに含まれる。この情報は、この実施例において利用されている移動局MS1の位置を発見するために、識別インジケータとして使用されてもよい。

【0066】

ここで、移動局は、移動電話1又は移動電話とコンピュータ2の統合ユニット以外に、ユーザに対して移動通信に関する可能性を提供する任意の種類の装置でよいことに注意すべきである。後者の配列は、しばしば「連絡機構（communicator）」と呼ばれることもある。他の適当な移動局の1例は、ページャ、即ちキャラクタ・ストリングを表示することができる「ビーパー（beeper）」である。重要なことは、移動局が所望の情報を受信及び／又は送信することができることであり、いくつかの場合において、特殊な認証シグナリング又は符号に代わるときにのみ、テキスト又は音声メッセージ形式も可能である。

【0067】

以上の例に加えて、アプリケーション45を2つの通信間をリンクさせるように配列して、アプリケーションにユーザを接続するために、2つの通信を使用することもできる。しかしながら、これは、他の何らかグループにより首尾よく達成され得る。例えば、ISP若しくは同様のサービス・プロバイダ、又は電気通信網のオペレータは、認証機関として機能し、かつ／又は2つの通信網間のリンクを提供すること、及び実際のアプリケーションに安全な接続を提供することができる。

【0068】

従って、本発明は、認証エリアにおいて重要な改良を達成できる装置及び方法

を提供する。本発明による配列は、それ自体公知の構成要素により実現するのが容易かつ経済的であり、また使用しても信頼性がある。本発明の以上の実施例は、付記する請求の範囲に記載された本発明の範囲を規制することを意図するものではないことに注意すべきである。従って、当該技術分野において習熟する者に明らかな全ての追加的な実施例、変更及びアプリケーションは、付記した請求の範囲に記述した本発明の精神及び範囲内に含まれる。

【図面の簡単な説明】

【図 1】

本発明を実施できる通信網のうちの 1 可能配列を概要図を示す。

【図 2】

本発明によりユーザを認証する一実施例の概要図である。

【図 3】

一可能移動局及び本発明の一実施例を概略的に開示する。

【図 4】

本発明の一実施例によるフロー・チャートを開示する。

【図 5】

本発明の一実施例によるフロー・チャートを開示する。

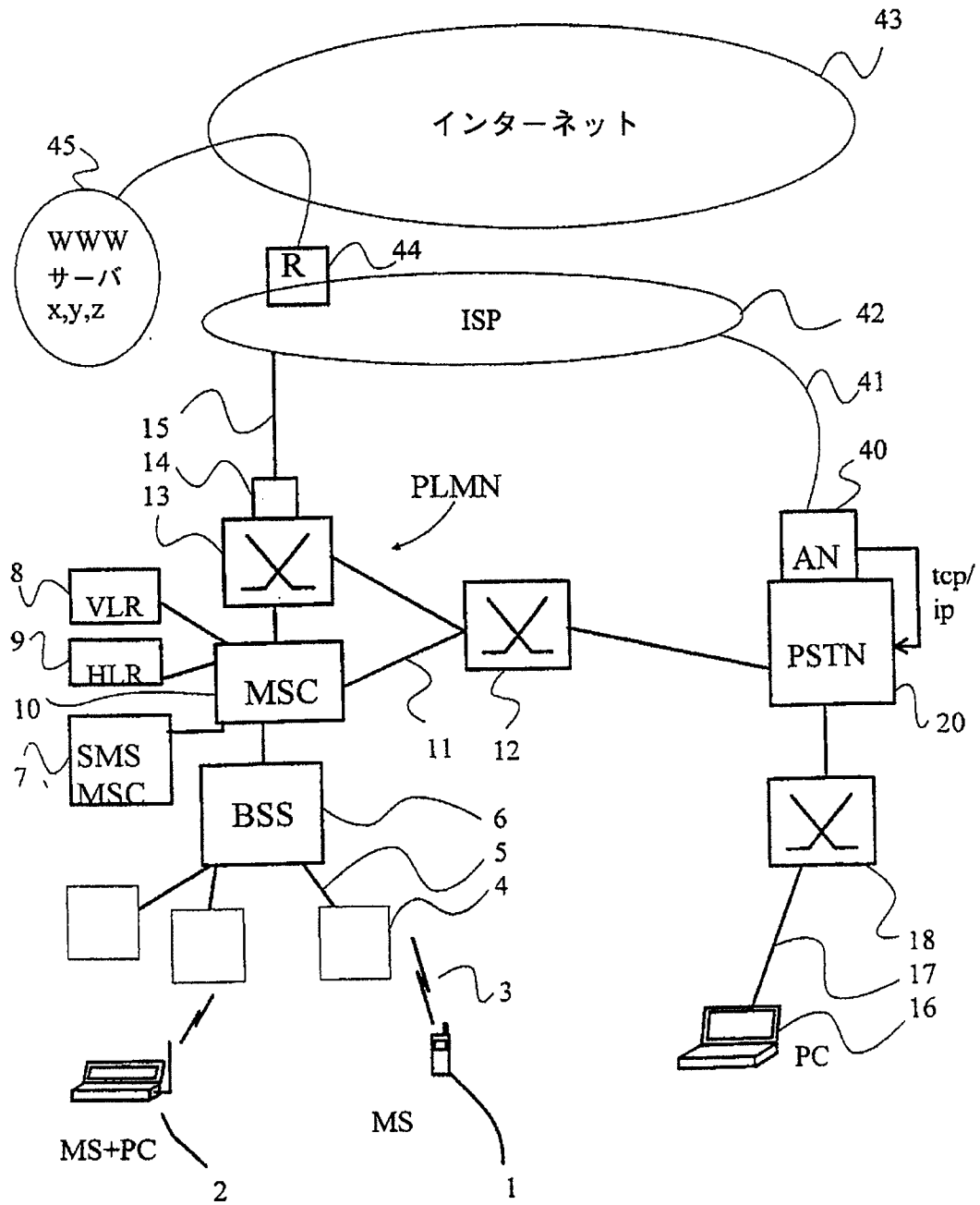
【図 6】

本発明による認証のための他の実施例を開示する。

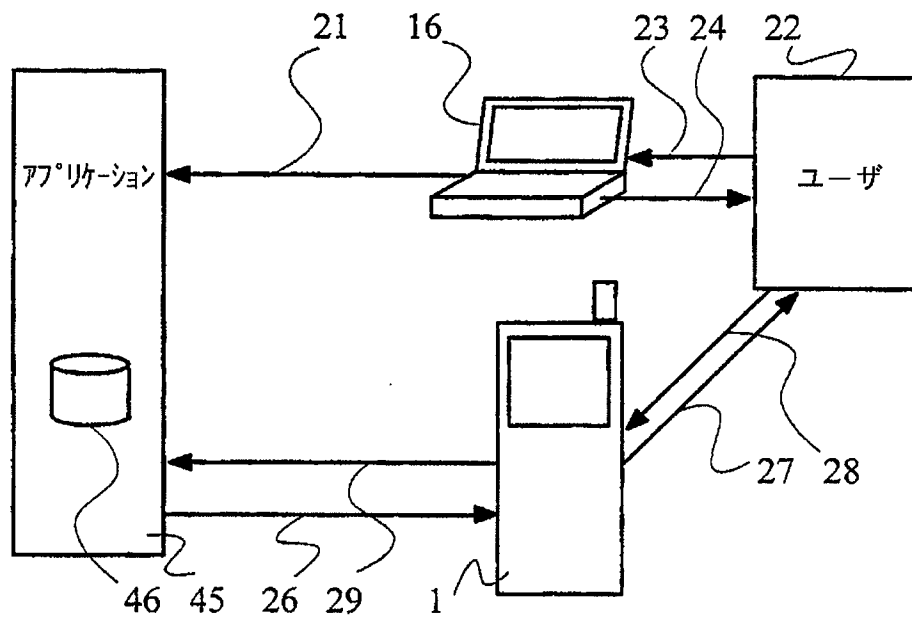
【図 7】

本発明の更なる実施例に関連する概要図である。

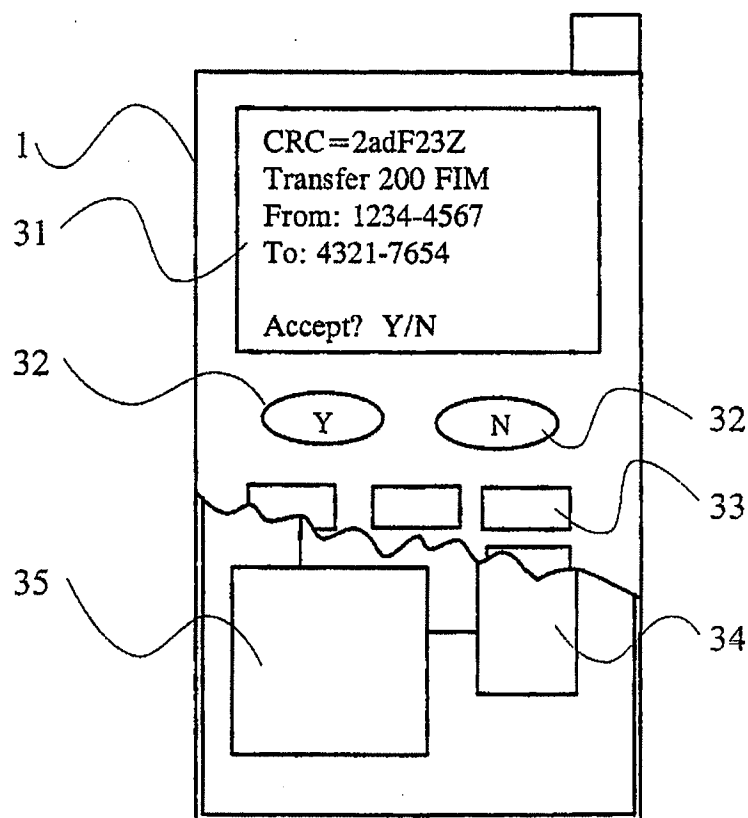
【図1】



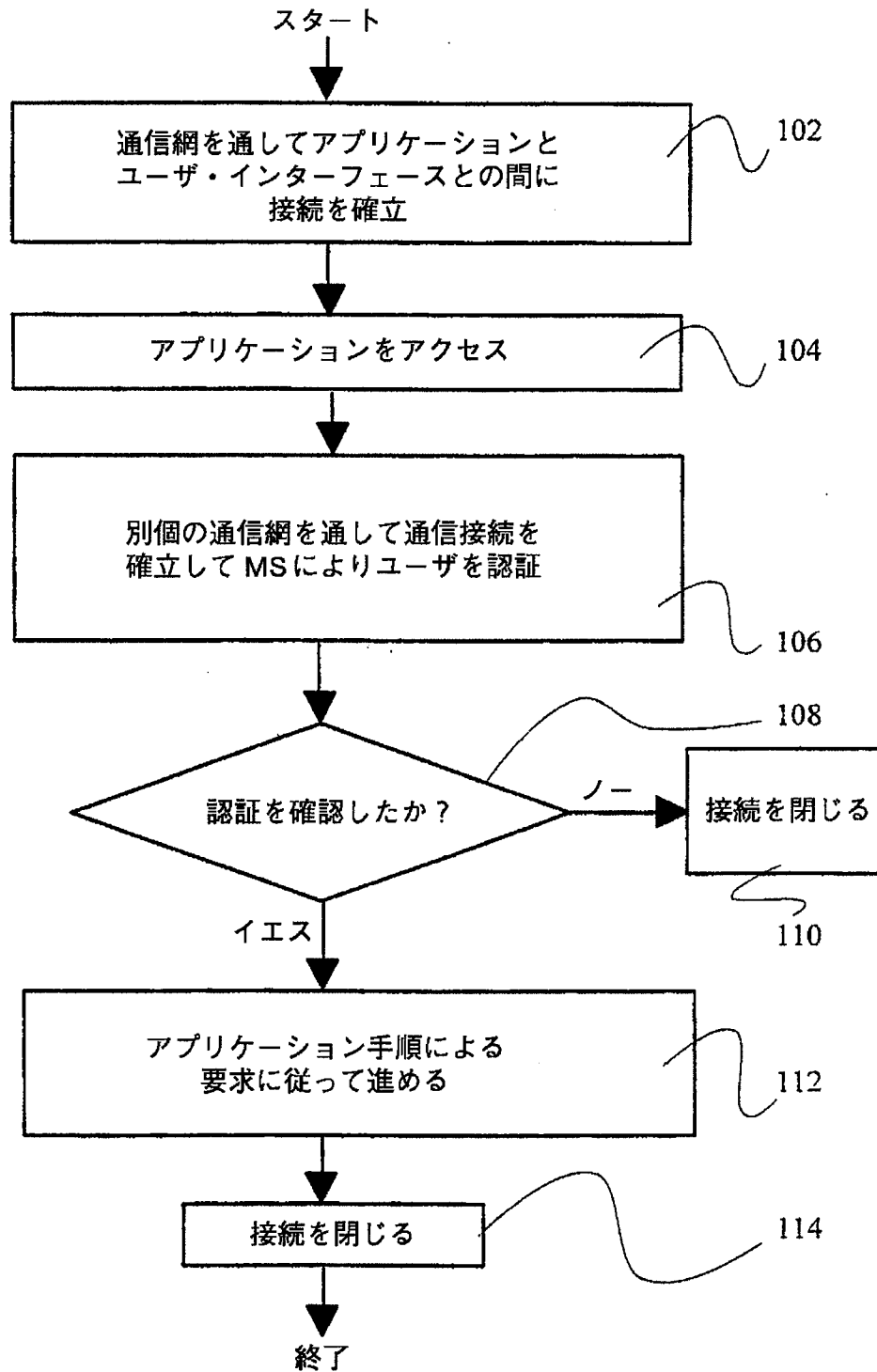
【図2】



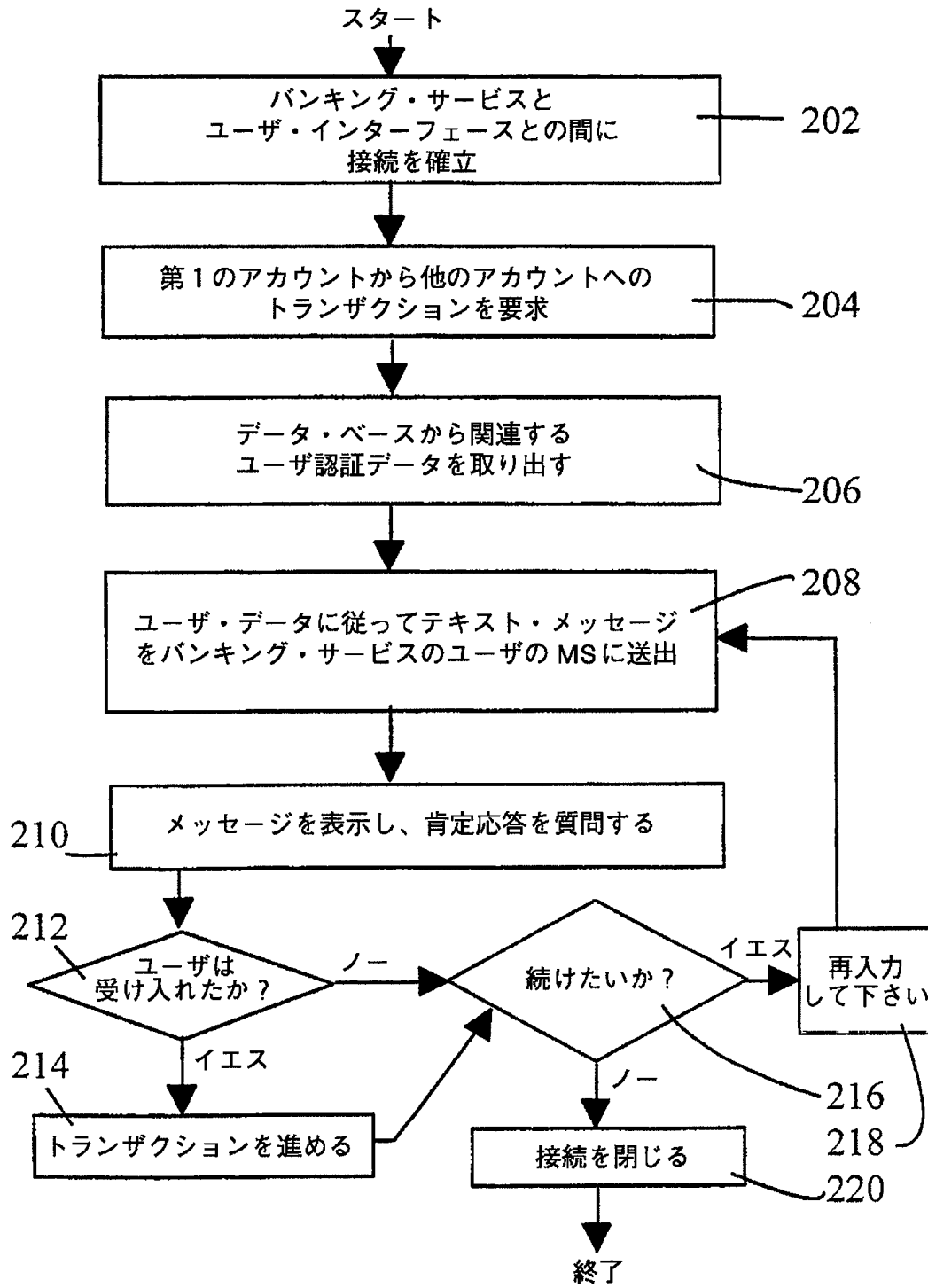
【図3】



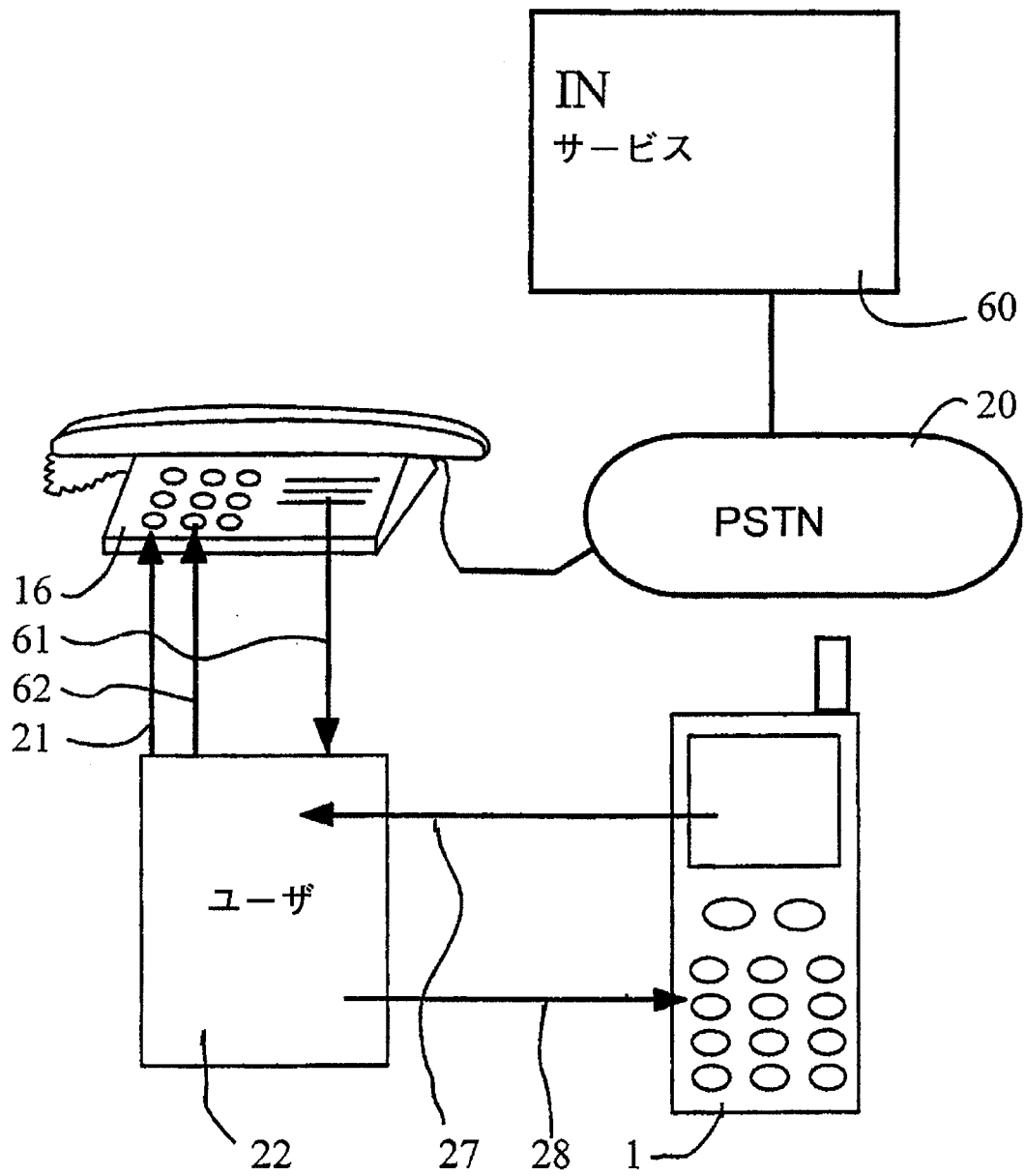
【図4】



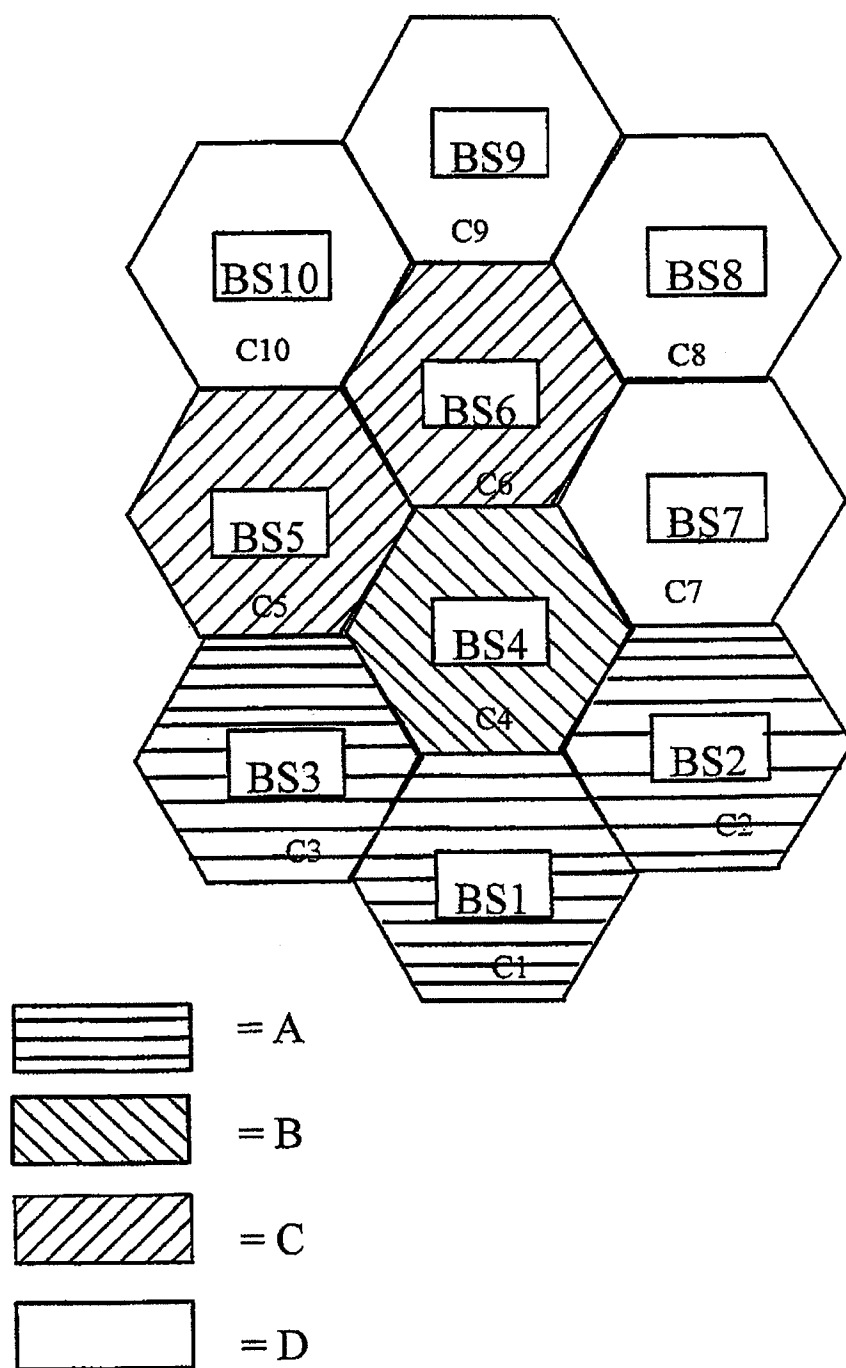
【図5】



【図6】



【图7】



【手続補正書】特許協力条約第34条補正の翻訳文提出書

【提出日】平成12年2月22日（2000. 2. 22）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正内容】

【発明の名称】 認証のための方法、配列及び装置

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】発明の詳細な説明

【補正方法】変更

【補正内容】

【発明の詳細な説明】

【0001】

（発明の属する技術分野）

本発明は、アプリケーションに対して認証を与える方法に関する。本発明は、更にアプリケーションに対して認証を与える配列、更に認証において使用される装置に関する。

【0002】

（発明の背景）

認証のために必要となる種々の電子アプリケーションが存在する。認証は、例えば、ユーザが特定のアプリケーションにアクセスしているとき、及び／又はユーザが既にアプリケーションを使用しているときに、要求されることがあり、またユーザを検証する、又はアプリケーションにいくつかの更なる処理を許容するユーザからの肯定応答を受け取るが必要となる。

【0003】

認証が必要になると思われるアプリケーション例は、インターネット、イントラネット即ちローカル・エリア・ネットワーク（LAN）、通信網を通してアク

セスされる支払い及び銀行サービス、リソース・アクセス、リモート・プログラミング、ソフトウェアの再プログラミング又は更新等のように、通信網を通して得られる種々の商業的なサービスを含む。通信網を通して得られるある種の無料サービスであっても認証を必要とすることがある。これらをアクセスしようとするユーザ（又サービスの使用中に認証をチェックする必要がある、若しくは使用中に何らか承認する必要がある場合を除き、これらを既に使用しているユーザ）の少なくともある程度の認証を必要とするサービス若しくはアプリケーションの量は、過去数年の間に非常に増大した。更に、認証の必要性は、将来、一層増大することも予想される。

【0004】

現在、通信の認証に関して既にいくつかの周知の解決法が存在する。通常、これらは、2つの通信コンピュータ装置間で種々の暗号化技術を使用する。基本的な認証シナリオによれば、前記2つのコンピュータ装置の暗号化機能に対してランダム・チャレンジ（random challenge）が与えられる。これらのコンピュータは共に、秘密（secret）即ち暗号鍵を有し、これは両コンピュータ内の暗号化機能にも与えられている。2つの暗号化機能の計算結果は、後で比較され、比較の結果が正となれば、その認証は有効であると見なされる。もし、比較が否定的な結果となれば、その認証テストは、失敗したと見なされる。

【0005】

更に、種々の既存の認証配列（arrangement）が既に存在する。米国特許第5,668,876号及びWO第95/19593号は、ページング・システム技術を使用することにより認証するいくつかの従来技術方法を開示している。従来技術の下記例について、そのいくつかの欠点の簡単な説明をする。即ち、

【0006】

パスワード。現在、1つのパスワード、又はいくつかのパスワードの使用は、認証のための最も頻繁に使用されるアプローチとなっている。このパスワードは、ユーザ・インターフェースを通して、例えば通信網に接続されたコンピュータ

端末を通してリモート・アプリケーションに与えられる。しかしながら、パスワードは網に対してアクセスを有する（及びパスワードを読み取るのに十分に熟練した）あらゆる者に曝されているので、この解決法は、網の脆弱性を考慮に入れていない。

【0007】

秘密。これは、例えばユーザ・インターフェースにより記憶されて使用される電子パスワード若しくは署名、又は暗号鍵として説明されてもよい。秘密が網に対して公開されていなくとも、結局は「悪行の手（wrong hand）」に渡り、本来、秘密のユーザであることを意図していた者以外のあるグループにより使用される恐れがある。

【0008】

ユーザ・インターフェース内の認証ソフトウェア。これは、認証に対してより複雑なアプローチである。パスワードは、ユーザ・インターフェース内のプログラムに与えられ、このプログラムが要求されたアプリケーションに対する暗号アクセスを自動的に認証する。これは、以上の解決方法より安全な配列を提供するとしても、依然としてユーザ・インターフェースからパスワードを捕捉する可能性が残っている。更に、実際のユーザに知らせることなく、ソフトウェアを変更することも可能である。

【0009】

スマート・カードとその関連のリーダー。スマート・カードは、暗号化された挑戦応答メッセージを通信することができるが、ユーザ自身からの認証を受け取るためのユーザ・インターフェースを内蔵していない。このようなインターフェースは、スマート・カード・リーダーに存在し得るが、このようなリーダーは、誤使用の可能性に対抗してうまく保護される必要があり、従って通常のユーザ（即ち、大多数のユーザ即ち公衆）は、通常、これらのリーダー・インターフェースに対して物理的なアクセスを有することができないが、これらは、スマート・カードを提供する組織を信用する必要がある。加えて、スマート・カード・リーダーは、互いに信用していない組織間では共有することができない。

【0010】

ユーザ・インターフェースを有するスマート・カード。これらは、既に存在するが、各安全プロセッサがそれ自身の安全ユーザ・インターフェースを有しなければならないので、高価になる。これらは、稀であり、その入出力機能は依然として極端に限定され、従って認証問題に対して経済的に適当な解決法であるとして保持されることはない。

【0011】

個別的な個人認証装置。このアプローチでは、ユーザがユーザ・インターフェースと個別的な認証装置との間の「通信手段」として使用される。従って、ユーザ・インターフェースは、ユーザが携帯認証装置（ポケット電卓のような装置）にタイプ入力する挑戦を受ける。認証装置は、応答として例えばある数を与えてもよく、従ってユーザは、この数をユーザ・インターフェースにタイプする。ここで、問題は、個別的な装置を購入し、携帯して使用する必要性に関係する。更に、いくつかの例では、通常、長く複雑なキャラクタ・ストリングを不正確にタイプ入力する可能性も存在する。

【0012】

以上は、既に、この認証システムを実施するときに係わり得るいくつかのグループについて述べている。以下、これらを更に詳細に説明する。

【0013】

ユーザは、通常、種々のアプリケーション又はサービスを使用する人間である。ユーザは、彼又は彼女のみが知っているパスワード（即ち秘密）（`public key method`：公衆鍵方法）により、又はユーザとアプリケーションとの間で共有される秘密（`secret key method`：秘密鍵方法）により、識別可能とされる。

【0014】

このアプリケーションは、ユーザの認証を保証したいグループである。更に、サーバと呼ばれるいくつかの場合においても、このアプリケーションを呼び出すことができる。アプリケーションの観点から、認証質問を4つの異なるカテゴリ（質問）に分けることができる。（1）は、その時点で他端にいるユーザか？（いわゆる対等者存在の認証（`peer-entity-authentication`）

ion)、(2)は、同一ユーザから更なるメッセージを受信しているのか？(メッセージ・ストリームの保全)、(3)あるユーザから発生している特定のメッセージか？(データ発生源認証)、及び(4)第3のグループであっても一定のユーザから発生していると思われるようなメッセージか？(非拒否)。

【0015】

ユーザ・インターフェースは、ユーザにアプリケーション又はサーバをアクセスできるようにする装置即ち配列である。大抵の場合、これを端末と呼ぶことができ、コンピュータ(例えば、パーソナル・コンピュータ、PC)、ワークステーション、電話端末、移動電話又は無線又はページャのような移動局、現金自動預払い機、及び／又はバンキング・マシン等のような装置からなるものでよい。ユーザ・インターフェースは、入出力機能を提供し、またアプリケーションの一部を提供することも可能である。

【0016】

個人認証装置(PAD)は、ユーザが自ら搬送するハードウェアのうちの1つである。PADは、いくつかの基本的な入力／出力機能、更にはいくつかの処理機能も有することができる。以上で述べたスマート・カード及び別個的な認証装置は、PADと見なされてもよい。大抵の場合に、ユーザは、そのPADを(殆ど)常時、携帯して、従って連続的に規制をしているので、ユーザは、そのPADに依存することができる。全ての可能パスワード即ち秘密は、これらを簡単な方法で明かせないようにハードウェアそのものに隠される。装置そのものは、ユーザとセキュリティ・プロセッサとの間の通信パスが危険にさらされないように、容易に変更できない。加えて、PADは、通常、記憶された状態の最小量を有し、プログラム自体も容易に変更できない。

【0017】

(発明の概要)

認証に関して、以上で述べた従来技術の解決方法が既に存在しているといえども、認証のエリア内で、以上で既に言及したものに加えて、まだいくつかの欠点が存在する。

【0018】

アプリケーションに対するアクセスが絶対的に安全、又は可能な限り安全にされている場合に、アプリケーションは、そのアーキテクチャーが容易に極端に複雑化することになり、また、アクセスして使用するために複雑化し、かつより時間が掛かるものとなる。セキュリティ・レベルを増加させれば、所要ハードウェア及びソフトウェアの量を増加させ、これがその保守及び更新のための必要性を増加させるに至り、従って、認証の総合コストは、高くなる恐れがある。複雑化及びコストは、セキュリティのレベルを下げることにより低減可能だが、これは通信が、十分でないセキュリティ・レベルに至ると予想される。加えて、技術的な進歩は、ハッカー達が最も複雑化したセキュリティ配列さえも解き明かすのを可能にさせるので、通信網において「絶対安全」条件さえも存在しないと信じる。

【0019】

人間の問題は、パスワード即ち秘密が極めて複雑かつ／又は長すぎる、又は沢山あり過ぎることになり得ることである。従って、ユーザはこれらを記憶するのが困難なことに気付くことになり得る。典型的には、秘密鍵方法において安全と見なされている秘密は、128ビットであり、また公衆鍵方法では1024ビットである。殆どの者は、この種の鍵を思い出すということが不可能である。

【0020】

加えて、ユーザは、外部装置なしに認証に必要とされる計算を実行することができない。以上で説明したように、基本的な認証は、しばしば挑戦及び応答の方法により行われる。これは、ユーザ（即ち、人間）が彼の秘密により、何らかのものを暗号化することが必要となる。これは、実際において続けていられない。

【0021】

今日の解決方法は、以上で説明したように、開放された通信網で伝送中にパスワード又は秘密を捕捉する可能性に加えて、いずれもユーザ・インターフェースの脆弱性に対して十分な注意を払っていない。端末装置は、複雑極まりない技術及びソフトウェアを開発したので、多くのユーザは、端末を十分に制御すること、又はその動作を理解することはもはや不可能である。加えて、多くのユーザが同一の端末装置（例えば、共通使用のPCである。）を共有すること、及び／又

は外部の保持要員が本質的に非公開機関のコンピュータに対するアクセスを有することがしばしば発生する。

【0022】

コンピュータ端末は、そのメモリ手段に、記憶された状態及びプログラムを備えており、これらは変更可能である。最近のコンピュータでは、ユーザがソフトウェアの変更に気付かないように、また物理的に装置そのものにアクセスすることなく、通信パスを通すように、そのソフトウェアを変更することさえも可能である。リスクの1例を挙げると、ユーザが例えばある銀行に送出するデータを変更するように、コンピュータがある日に全ての銀行間の振替をユーザ（利用者）により指定されていたもの以外の他の預金口座に変更するように、コンピュータ端末内のプログラムを変更することも可能である。通告のないこの変更又は再プログラミングは、通常の個人的なユーザに対して使用されたとき、特に会社又は公的な機関のような組織に対して使用されたときは、深刻かつ莫大な損害を発生させる恐れがある。これは、全て通常の端末装置及び通信パスが信頼されないことを意味する。

【0023】

従って、本発明の目的は、従来技術の解決方法の欠点を克服すると共に、認証に対して新しい形式の解決方法を提供することである。

【0024】

更に、本発明の目的は、アプリケーションをアクセスしたいユーザを従来技術において可能であったものより安全な方法により認証することができる方法及び配列（arrangement）を提供することである。その目的は、認証の必要性が既にアクセスしたアプリケーションの使用中に発生したときに、認証を与えることである。

【0025】

本発明の目的は、認証において移動局を利用することができる方法及び配列を提供することである。

【0026】

本発明の追加的な目的は、認証において移動局の識別モジュールを利用するこ

とができる解決方法を提供することである。

【0027】

本発明の他の目的及び効果は、添付図面に関連させた明細書の下記部分により達成される。

【0028】

これらの目的は、通信網を通して供給されるアプリケーションに認証を与える新しい方法により得られる。本発明によれば、通信網を通して提供されるアプリケーションに対してユーザのアクセスを可能にさせるように、アプリケーションと通信網を通るユーザ・インターフェースとの間の接続が確立される。更に、第2の通信網を介するアプリケーションと移動局との間の接続が確立される。アプリケーションに対する認証は、アプリケーションと通信する移動局により、第2の通信網を介して与えられる。

【0029】

更なる一実施例によれば、認証方法は、通信網を通して提供されるアプリケーションに対してユーザがアクセスできるように、アプリケーションと通信網を通るユーザ・インターフェースとの間に接続を確立するステップを含む。前記アプリケーションに対する認証は、認証の暗号処理において移動局の加入者識別モジュール（Subscription Identification Module：SIM）の秘密を利用するように、移動局により提供される。

【0030】

本発明は、更に、通信網を通してアプリケーション・プロバイダにより提供されるアプリケーションに対する認証を与える配列を含む。この配列は、アプリケーションを使用できるように、アプリケーションと前記通信網を通るユーザ・インターフェースとの間の接続とを含む。この配列は、更に、認証を可能にするように、第2の通信網を介する、アプリケーションと移動局との間の第2の接続とを含む。この配列は、更に、第2の通信網を介して、アプリケーションに対してユーザを認証する手段を含む。

【0031】

他の実施例によれば、本発明は、通信網を通して提供されるアプリケーション

に対して認証を与える移動局を備え、このアプリケーションは、通信網に接続されたユーザ・インターフェースによりアクセスされ、かつ前記移動局は、通信のためにユーザ・インターフェース以外の異なる通信網を使用し、移動局は、ユーザ・インターフェースによりアクセスされる前記アプリケーションの使用を認証するために使用される。

【0032】

この解決方法は、認証に対して信頼性のある新しい方法を導入しているので、本発明によりいくつかの効果が得られる。本発明の認証方法及び配列は、余分な代替又は追加的な装置なしに、既存の通信網に容易に実施できる。この配列は、実際において、ある種の認証を必要とする通信システムを通じて提供される任意のアプリケーションと関連して、異なる種々のアプリケーションとの接続に使用されてもよい。

【0033】

ユーザは、別個の認証装置（PAD）又は異なる多くの認証装置を搬送することから開放される。更に、ユーザは、通常、移動局が常にユーザと共にあり、かつユーザがこれらの移動局をよく管理する傾向があるので、本発明による個人認証装置（Personal authentication device：PAD）を信頼することができる。加えて、例えば窃盗の移動局の場合は、移動電話加入者及び／又はそのSIMをオペレータにより容易に取り消すことができる。移動局の全ての秘密は、これらを容易に明かさないように、そのハードウェアに首尾よく隠されている。加えて、移動局の装置自体は、ユーザとセキュリティ・プロセッサとの間の通信パスを危険にするように容易に変更され得ない。

【0034】

システムは、最小量の記憶状態を含み、かつプログラムは容易に変更され得ない。移動局の既存SIM、より具体的に、その秘密は、必要とする暗号化手続に利用されてもよい。従って、SIMは、新しい目的用のセキュリティ・カードとして利用されてもよく、また、虚偽の疑いがあれば、SIMの使用を制御する既存のパーティ、即ち直ちにSIMを取り消すことができる移動電話網のオペレータが存在する。

【0035】

以下、添付図面を参照して本発明及び他の目的、並びにその効果を添付図面を参照して複数例により説明するが、種々の図面を通して同一参照番号は、同一の機能を表している。本発明の以下の説明は、本発明をその接続により提供された特定形式に限定されず、それよりも本発明は、付記する請求の範囲の精神及び範囲に含まれる全ての変形、類似性及び代替を包含することを理解すべきである。

【0036】

(発明の詳細な説明)

図1は本発明を実施するときに使用することができる一つの網配列の概要図である。図1の配列は、20により表すブロックとして概要的に示されている公衆交換電話網(Public Switched Telephone Network: PSTN)を含む。例示したPSTNは、固定回線電話網(又はプレーン旧電話サービス(Plain Old Telephone Service: POTS))であって、これは、アプリケーションをアクセスできるようにユーザ・インターフェース16を可能にする通信網を形成する。この実施例によれば、ユーザ(図示なし)は、インターネット接続を通して得られるWWWサーバ45のうちの1つにより所望のサービスにアクセスするように、ユーザ・インターフェースとして、PSTNに接続されたユーザ・インターフェース16を使用することができる。開示された端末16は、パーソナル・コンピュータ(PC)であるが、しかし更にワークステーションのように他の形式のユーザ・インターフェース、現金自動預払い機等を使用することもできる。

【0037】

更に、公衆地上移動電話網(Public Land Mobile Network: PLMN)を開示する。これは、例えば、セルラ電話網又は同様の移動通信システムであってもよい。更に、移動局MS1及びMS+PC2も開示する。MS+PC2は、統合された移動電話及び携帯コンピュータとして定義されてもよい。これらは共に、エア・インターフェース3を通して、PLMNのいくつかの基地局(BS)4のうちの一つを通るPLMNと通信することができる。

【0038】

PLMNの1形式は、ETSI (European Telecommunications Standard Institute: 欧州電気通信標準委員会) によるGSM提唱においてよく規定されているデジタルGSM網 (Global System for Mobile communication : GSM: 移動体通信グローバル・システム) であり、その網構成自体は、推奨GSM01.02若しくはGSM03.02、又はその改訂版に詳細に記載されている。本発明は、主としてGSMの技術用語を使用して例示的なセルラ電話網に関連して説明されていることに注意すべきであり、当該技術分野において通常に習熟する者は、この発明を任意の移動システムに実施できることを理解すべきである。更に、明確にするために、例示的なシステムの動作を説明する目的のために、必要と考えられる移動電話網構造の複数部分のみが示されていることに注意すべきである。習熟する者は、電話網が通常、説明したものより必要とする他の装置を含めてもよいこと、PLMN又はPSTNの開示したいくつかの要素が省略又は他のなんらかの形式の複数要素により置換されてもよいこと、及び多数の移動電話網及び通常の固定地上回線網が互いに協同し、かつ交換してもよいことに確かに気付く。習熟する者は、インターネットに対する接続が如何なるPSTN、又はユーザ・インターフェース16とインターネット43との間における同様の網構成のない、直接接続であってもよい。しかしながら、これらの代替は、当該技術分野において通常に習熟する者に知られているので、更に詳細に示し、また説明もしていない。

【0039】

公衆地上移動電話網 (PLMN) に基づくGSMは、通常、いくつかの移動サービス交換局 (mobile service switching center: MSC) 10を含む。続いて、これらはそれぞれが複数の基地局サブシステム (BSS) 6 (明確にするために1MSC及びBSSのみが示されている。) に接続される。基地局サブシステム6は、通常、基地局コントローラBSC及び必要とするインターフェース装置を含み、かつ複数の基地局 (BS) 4に接続され、それぞれはセルと呼ばれるある地理的なエリアを管理する (セルについては、図7を参照)。

【0040】

図1の移動サービス交換局10は、更に、交換12及び回線11を通して公衆交換電話網（PSTN）20に接続又はリンクされる。更に、MSC10は、例えば、（番号43により指示された）インターネットであるグローバル通信網にも接続される。MSCは、総合デジタル通信網（ISDN）又は適当な他の形式の通信網に接続されてもよい。異なる電気通信網システムの異なる構成要素間で必要とするリンクは、それ自身が当該技術分野において周知である。

【0041】

PLMNは、更にデータ・ベース、MSCに接続されたいわゆるホーム位置レジスタ（home location register：HLR）9を含む。移動電話網の加入者であるこれらの移動端末1及び2は、HLR9に登録される。各ローカル移動電話交換局10は、更に、訪問者位置レジスタ（visitor location register：VLR）8と呼ばれる各ローカル・データ・ベースを含み、これには、任意の与えられた時点で移動電話がそのローカル移動電話サービス交換局MSCにより処理されるセルのうちの1つのエリア内に位置した全ての移動局1及び2が登録される。

【0042】

移動局は、通常、これらの移動局のそれぞれ内に搭載された、そうでなければこれに物理的に接続されたSIM（Subscriber Identification Module：加入者識別モジュール）により識別される。SIMは、情報及び秘密に関係した種々のユーザ（加入者）を含むモジュールである。これは、更に、無線通信の暗号化に関係する情報を含めてもよい。SIMは、移動局に固定的に又は削除可能にアセンブリされてもよい。本発明におけるHLR及び／又はVLRレジスタと共に、SIMの利用を以下、この明細書において更に詳細に説明する。

【0043】

以上で説明したように、ユーザは、固定若しくは移動電話網を通して、又は直接接続を通してインターネット43に接続されてもよい。しかしながら、例えばGPRS（General Packet Radio System：汎用パ

ケット無線システム)に関係するときに、接続間にはいくつかの相違が存在し得るが、しかしインターネット網のサービスは、PSTN及びPLMNシステムの両ユーザに利用可能である。この例では、PSTN20と共に移動通信交換局(MSC)10がアクセス・ノード(AN)14及び40により、マルチプロトコル・インターネット43に対してアクセスが提供される。1通信網当たり1ANのみであっても、実際において、ANの数が本質的に更に大きくされてもよく、更にAN数が連続的に増加していることが理解される。一解決方法によれば、信号をデータ・パケットに変換することができる特殊なインターネット・アクセス・サーバIASがインターネットに向けてのANとして使用される。

【0044】

インターネット43のユーザは、ユーザ端末1、2又は16からインターネットに対して通信接続を行うインターネット・サービス・プロバイダ(Internet Service Provider:ISP)42との接続を行った。ユーザがインターネット接続をしたいときは、ユーザがその所望のアドレス(いわゆるインターネット・プロトコル・アドレス)にユーザの端末16に接続するように、インターネット・サービス・プロバイダ(ISP)42に対して呼出しをする。呼の接続は、PSTN20により確立されて、少なくともローカル交換18を通して、多分、トランク回線(図示なし)を通して接続又は相互接続される一又はいくつかのトランジット交換を通る。図1は、両通信網がインターネットに向かって通信する唯一のISPのみを開示しているが、通信は異なるISPを通るように配列されてもよいことを理解すべきである。

【0045】

図1は、更に、異なるサービスを提供するサーバ・データ・ベースx、y及びzを含むWWWサーバ45(World Wide Web server:ワールド・ワイド・ウェブサーバ)を開示している。これはISPからルータ44を通り、インターネット43を通る前記サーバ45への接続を開示している。サーバは、認証を必要とするバンキングサービス、電子ショッピング・サービス等のように、任意の通信網を通して得られる任意のサービスであってもよいことを理解すべきである。

【0046】

移動局1（又は2）は、ユーザがユーザ・インターフェース16を介し、PSTN20を通してWWWサーバ45により提供されるサービスxにアクセスするとき、又は既にアクセスしたときに、個人認証装置（personal authentication device：PAD）として使用される。移動局1は、チャンネルが実際のユーザ・インターフェース16により使用されるよりも、別個の通信パス即ちチャンネルを通してサービスxと通信する。移動局は、通常、ユーザがこれを常時、保持しているので、信頼できるとされる。移動局及び通常のPADに対する人間工学及び機能的な必要条件是、本質的に同一であり、MSはPADに適したユーザ・インターフェースを有する。最近のMSは、認証目的に適したセキュリティ・プロセッサ・インターフェースさえも有する。

【0047】

移動局による認証を達成するいくつかの代替があり、ここで、その複数例を以下で更に詳細に説明する。

【0048】

ここで、図2及び4を参照する。図2は認証のための1配列、また図4は基本的な実施例による動作のフロー・チャートを概略的に開示している。ユーザ22は、通信網（図2における矢印21、図4におけるステップ102及び104）により確立された接続を通るバンキング・サービスのように、所望のアプリケーション45にアクセスする要求をユーザ端末16により送出する。アプリケーション45は、データ・ベース46を含んでもよく、又は図1のMSC10のHLR9のように、別個のデータ・ベースに接続され、これによりアプリケーションは、必要とするユーザ情報を抽出できるようにされる。この情報に基づいて、アプリケーションは、認証目的のためにユーザ22の移動局1に対する接続を確立する（矢印26、ステップ106）。この段階で、ユーザは、移動局1を使用して、アクセスが許可され、かつサーバの実際の使用を開始できることを表す確認信号29（即ち、肯定応答）を返送することにより、ユーザ・インターフェース16により作成した接続21を受け付けることができる（ステップ108及び112）。例えば、アプリケーションがMS1に到達できないことに基づき、認

証失敗の場合は、全ての接続が閉鎖される（ステップ110）。代替として、ユーザが直ちに又はある時間後にアクセスを再試行するのが許可されても、又はユーザが失敗した認証のためにユーザ・インターフェース16によりいくつかの追加的な措置を取るように指令されてもよい。

【0049】

認証又は肯定応答機能を実行する方法は、PLMNの短メッセージ・システム（SMS）の短メッセージを使用することである。GSMシステムにおいて、移動局へ及びからの短メッセージを送出するために、図1に7により表されているSMS MSC（SMS Message Service Center：SMSメッセージ・サービス・センタ）が設けられる。以上で説明し、かつ言及した仕様により定義されたように、同一の網構成要素を使用して、サービス・センタ7は、移動電話加入者にメッセージを送出する。SMSメッセージ・シグナリングは、通常、例えば受信機識別、送出情報、タイム・スタンプ等を含む。

【0050】

図3は、移動局MS1がSMSメッセージを受信した一解決方法を開示している。このための方法ステップは、図5のフロー・チャートにより示されている。この実施例によれば、ユーザは、ユーザ・インターフェース16を通してバンキング・サービスをアクセスした後に、200FIMの和がアカウントNo. 1234-4567からアカウント4321-7654に振替されるべきことを要求した（ステップ204）。従って、アプリケーションは、適当なデータ・ベースからユーザ関連の認証データを取り出し（ステップ206）、かつ移動局1にテキスト・メッセージを送出する（ステップ208）。MS1は、図示のようにテキストを表示し、ユーザに、「イエス」又は「ノー」キーをそれぞれ押すことによりトランザクションを肯定又は否定するように、質問をする（ステップ210）。次いで、応答がアプリケーションに返送されて、「イエス」の場合は、トランザクションが進み（ステップ214）、「ノー」の場合は、他のいくつかの処置を取る。

【0051】

更に、図2の矢印27と28がMS1及びユーザ2が通信する段階を示してお

り、MS 1のディスプレイ 3 1で見ることにより受信される情報が矢印 2 7により示され、ユーザによりMS 1に与えられる応答が矢印 2 8により示されている。説明したように、ユーザは、MSのY又はNキー 3 2を押すことにより、適正な選択を選択できる。従って、ユーザが受け取った即ちトランザクションに「署名」した場合は、バンキング・サービスが進む。ユーザがトランザクションを確認しない即ち「ノー」キーを押した場合は、アプリケーションは、ユーザ・インターフェースに訂正、取り消し、新しい宛先アカウント等を入力するように要求することができる（ステップ 2 1 6、2 1 8）。

【0052】

ある期間内でアプリケーションが応答を受信しない、又は応答がいずれにしろ誤っている場合は、アプリケーションは、確認、又は全ての接続を閉鎖するための第2の要求を送出することができる。

【0053】

ユーザは、次のいくつかのトランザクション、更には一旦アプリケーションをアクセスした後に他のいくつかのバンキング・サービスをも処理することができる。ステップ 2 1 6において、ユーザが最終的にユーザ・インターフェース 1 6に対して、ユーザが継続したくないことを応答するときは、接続が閉鎖される（ステップ 2 2 0）。

【0054】

本発明の一実施例によれば、本発明の認証配列を実施する際に、図 1のPLMNのHLR、更にはVLRに含まれる情報を利用することができる。これは、移動電話加入者のそれぞれが、図 1のHLR 9内に、位置情報（VLR番号）、基本電気通信サービス加入者情報、サービス規制及び補助サービス等と共に、既に述べたSIM（加入者識別モジュール）、IMSI（International Mobile Subscriber Identity：国際移動電話加入者識別）、及びMSISDN（Mobile Subscriber ISDN Number：移動電話加入者ISDN番号）に関連した情報を含むということにより、可能にされる。

【0055】

従って、更に、MS 1内に挿入されたSIM (Subscriber Identification Module: 加入者識別モジュール) カード34を開示する図3を見ることができる。電話会社は、通常、ユーザの支払い及び位置を制御するためにSIMを使用する。従って、SIMカード34は、使用状態にして、電話呼出をする前に、MS 1に接続される必要がある。図3のMS 1は、更にMS PADコントローラ35 (Mobile Station Personal Authentication Device controller: 移動局個人認証装置コントローラ) を含む。本発明では、これらにより、SIM 34は、ユーザを識別し、かつ／又は一秘密又はいくつかの秘密を含む手段として使用されてもよく、またMS PADコントローラ35は、認証処理を制御するために使用される。コントローラ35は、認証手順の一般的な制御に加えて、例えば種々の暗号化処理に関連する全ての計算を行うように配列されてもよい。認証手順において、MS PADコントローラ35により制御されるSIM 34を利用することができる配列は、種々である。

【0056】

SMSサービスを利用する前述の配列の代わりに、トランザクションは、更に、例えば電子的なトランザクションにより支払われるバンキング・サービス又は他の商業的なサービスのようなアプリケーションがMS PAD35に対するトランザクションの詳細をMS PAD35に移動電話網を通るデータ信号として送出するように、肯定応答されてもよい。信号の正しさは、予め定めたアルゴリズムに従い、かつSIM34の秘密を利用して、MS PAD35により計算されたチェックサムにより保証されてもよい。即ち、チェックサムは、ユーザ端末16により表示されたサムと一致する必要がある。ユーザがトランザクションを受け入れると、ユーザは、これに肯定応答をし、かつ（例えば、公衆キー暗号化及び無拒否の使用を必要とするときに）ユーザの秘密を使用する、又はアプリケーションと共用される秘密を使用することにより、アプリケーションからのメッセージ信号26に「署名」するように、MS PAD35に対して許可を与える。その後、アプリケーションは、ユーザ・インターフェースによる要求に従って進行する。一実施例によれば、更に、SIM34の秘密又は複数の秘密は、メッ

セージの暗号化、及び／又はアプリケーションとMSとの間のシグナリングに使用されてもよい。

【0057】

図6は図2に対する他の実施例を開示する。この実施例において、ユーザ・インターフェース16は、それ自体が公知の方法によりPSTN20に接続された通常の電話端末の形式にある。PSTNは、更にこの実施例においてアプリケーションを形成するインテリジェント・ネットワーク・サービス(intelligent network service:IN)60に接続される。移動局1は、図3に関連して以上で説明したPADコントローラ35及びSIM34を含む。一実施例によれば、与えられたサービスに対するサービス識別子と個人秘密を含むMS PAD対がPADコントローラ内に記憶される。これらの対は、例えば以下の方法で使用される。

【0058】

ユーザは、サービスに対する電話呼を確立することにより、前記INにサービスをアクセスする(矢印21)。アプリケーションは、音声メッセージとして与えられた番号により、又は前記電話端末上の可能ディスプレイにより、ユーザに挑戦する(矢印61)。この挑戦において、ユーザは、キーパッドによりMSに対して、特定の番号と一緒にキー入力し(矢印28)、その後、PADコントローラは、更なる番号のつながりを受信するように、好ましいアルゴリズムに従って必要な計算達成する。この計算において、特定のユーザのためにSIMに記憶した秘密は、アルゴリズムの一部を形成することができる。この秘密は、アプリケーション特定秘密又はPLMNの秘密であり得る。次いで、計算の結果は、ユーザ・インターフェース16に供給され(矢印62)、PSTN20を通る質問によりINサービスに送信される。これが期待した値と一致した場合は、INサービス60は、ユーザが固定回線端末16によりこれを使用するのを許可する。

【0059】

以上で述べた実施例は、例えば通常的な任意のPOTS回線電話を通して得られる電話呼出又はサービスを支払うときに、使用されてもよい。例えば、これは、任意の電話端末による呼が移動電話加入者から(即ち、特定のSIMカードの

所有者から）課金される配列を可能にする。移動電話加入者は、例えば移動電話により発生した呼が通常のPOTS電話による呼よりも高価となる場合、又はMS1がユーザが正しい無線接続を確保できる移動電話網のエリア内に存在しないときに、このサービスが有用なことが解る。

【0060】

追加的な一実施例（図示なし）によれば、移動局1及びユーザ・インターフェース16は、無線接続、赤外線接続、又は必要なカップリングによる固定管路接続のような適当な運用上の接続により、相互に直接通信することができる。これは、MS1とユーザ・インターフェース16との間の「リンク」として動作しているときに、ユーザが犯すかも知れないタイプ誤りの危険性を軽減する。

【0061】

一つの代替によれば、移動局は、1以上のSIMカード34を受け入れるように配列される。これにより、異なる認証目的に1移動局を使用することができる。例えば、ユーザは、異なる3つのSIM、即ち、ユーザの作業に必要とされる認証用に一つ、個人用に一つ、及び更なる必要性のため、例えば「協会の議長」用に一つを備えることができる。これらのSIMはそれぞれ、それ自身の電話番号、アラーム・トーン等を有することができる。

【0062】

更なる代替によれば、MS1はPLMNを通してアプリケーションと通信し、かつこの通信に必要とするメッセージ及び／又はシグナリングがSIMの秘密又は複数の秘密を使用して暗号化される。これは、SIMの秘密が固有なときに、唯一の通信網、即ちPLMNのみを使用して安全通信を可能にさせ、また第3のグループがシグナリングに含まれている情報を得ること、又はシグナリングに割り込むことが不可能となる。

【0063】

ここで、図1及び7を参照して本発明の更なる実施例を説明する。図7は複数の連続的な無線サービス・エリア、即ち複数のセルに分割された任意の地理的領域の概要セル・マップを開示する。図7のシステムは、10セル（C1～C10）のみを含むように示されているが、セルの数は、実際にはもっと多数となり得

る。1 基地局がセルのそれぞれに関連され、かつその内部に配置される共に、これらの基地局がそれぞれBS 1～BS 10と表されている。これらの基地局は、基地局サブシステム（図1のBSS 6）に接続されている。更に、1セルは、1又はいくつかの基地局をカバーしてもよい。これらのセルは、4グループA～Dにグループ分けされ、各グループは、対応するマーキングによりマークされているように、1以上のセルを含むことができる。

【0064】

各グループは、異なる4セル・カテゴリA～Bを設けるように、システムによって1ユニット即ち1エリアと見なされる。その目的は、これらのセルを異なる複数の認証カテゴリ、即ち複数のクラスに分割できることを示すことにある。その背景の概念は、ユーザがある予め定めたセル・エリア内に位置していない場合に、認証データ・ベース内の認証データは、ユーザにアプリケーションをアクセスするのを許可しない規制を含めてもよいということである。例えば、会社が認証に関して被雇用者のMSを使用するときは、認証の可能性を規制してその会社の事務所の近傍にあるセル内（例えば、エリアA内）のみで許容するように、エリアを制限することができる。

【0065】

以上は、図1内の8により表された訪問者位置レジスタVLRにより、容易に実施可能である。MSCのエリア内をローミングしている複数の移動局（MS）1又は2は、そのエリアに対して責任を持つVLR 8により管理される。VLR 8は、MS 1又は2が位置エリアに出現するときは、VLRは更新手順を開始する。更に、VLR 8は、例えばMSが、IMSI、MSISDN、及び例えばGSM 09.02仕様に従って登録される位置エリアを含むデータ・ベースも有する。いわゆるセル・グローバル識別は、更に、セル識別を含み、かつMS 1とMSC 10との間のメッセージに含まれる。この情報は、この実施例において利用されている移動局MS 1の位置を発見するために、識別インジケータとして使用されてもよい。

【0066】

ここで、移動局は、移動電話1又は移動電話とコンピュータ2の統合ユニット

以外に、ユーザに対して移動通信に関する可能性を提供する任意の種類の装置でよいことに注意すべきである。後者の配列は、しばしば「連絡機構（communicator）」と呼ばれることもある。重要なことは、移動局が所望の情報を受信及び／又は送信することができることであり、いくつかの場合において、特殊な認証シグナリング又は符号に代わるときにのみ、テキスト又は音声メッセージ形式も可能である。

【0067】

以上の例に加えて、アプリケーション45を2つの通信間をリンクさせるように配列して、アプリケーションにユーザを接続するために、2つの通信を使用することもできる。しかしながら、これは、他の何らかのグループにより首尾よく達成され得る。例えば、ISP若しくは同様のサービス・プロバイダ、又は電気通信網のオペレータは、認証機関として機能し、かつ／又は2つの通信網間のリンクを提供すること、及び実際のアプリケーションに安全な接続を提供することができる。

【0068】

従って、本発明は、認証エリアにおいて重要な改良を達成できる装置及び方法を提供する。本発明による配列は、それ自体公知の構成要素により実現するのが容易かつ経済的であり、また使用しても信頼性がある。本発明の以上の実施例は、付記する請求の範囲に記載された本発明の範囲を規制することを意図するものではないことに注意すべきである。従って、当該技術分野において習熟する者に明らかな全ての追加的な実施例、変更及びアプリケーションは、付記した請求の範囲に記述した本発明の精神及び範囲内に含まれる。

【図面の簡単な説明】

【図1】

本発明を実施できる通信網のうちの一可能配列の概要図を示す。

【図2】

本発明によりユーザを認証する一実施例の概要図である。

【図3】

一可能移動局及び本発明の一実施例を概念的に開示する。

【図４】

本発明の一実施例によるフロー・チャートを開示する。

【図５】

本発明の一実施例によるフロー・チャートを開示する。

【図６】

本発明による認証のための他の実施例を開示する。

【図７】

本発明の更なる実施例に関連する概要図である。

【手続補正書】特許協力条約第34条補正の翻訳文提出書

【提出日】平成12年4月17日（2000. 4. 17）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 アプリケーションのためにユーザを認証する方法であって、アプリケーションが第1の通信網を通してユーザに利用可能な方法において、ユーザがアプリケーションをアクセスできるように、前記第1の通信網を通してアプリケーションとユーザ・インターフェースとの間に接続を確立し、移動局が登録されているデータ・ベースに接続可能なアプリケーションと、移動局との間に第2の通信網を通して接続を確立し、かつ第2の通信網を通してアプリケーションと通信する移動局によりアプリケーションに対するユーザを認証する方法。

【請求項2】 認証のステップは、ユーザがユーザ・インターフェースによりアプリケーションをアクセスするときに、移動局を使用してユーザの識別を検証することを含む請求項1記載の方法。

【請求項3】 認証のステップは、移動局を使用して、ユーザがユーザ・インターフェースを通してアプリケーションから前に要求したトランザクション又は処置に肯定応答することを含む請求項1記載の方法。

【請求項4】 認証のステップは、移動局の加入者識別モジュール（SIM）の秘密が認証の暗号化処理に利用されるように、移動局を使用することを含む請求項1記載の方法。

【請求項5】 移動局はセルラ電話であり、かつ第2の通信網は、デジタル・セルラ網を含む前記請求項のうちのいずれかに記載の方法。

【請求項6】 移動局の加入識別モジュール（SIM）の秘密を利用して認

証ステップに関連したシグナリングを暗号化することを含む前記請求項のうちのいずれか一つに記載の方法。

【請求項 7】 移動局の加入識別モジュール（SIM）は、ユーザの識別を提供するために使用される前記請求項のうちのいずれか一つに記載の方法。

【請求項 8】 ユーザ・インターフェースからアプリケーションへの接続のコストを SIM により識別された加入の保持者に請求するステップを含む請求項 7 記載の方法。

【請求項 9】 アプリケーションと移動局との間のシグナリングの少なくとも一部は、短メッセージ・システムの形式にあるテキスト・メッセージである前記請求項のうちのいずれか一つに記載の方法。

【請求項 10】 認証手順の 1 パラメータとして移動局のエリア位置情報を使用するステップを含む前記請求項のうちのいずれか一つに記載の方法。

【請求項 11】 通信網を通してアプリケーション・プロバイダにより提供されるアプリケーションに対してユーザの認証を与える配列において、

ユーザ・インターフェースと、

アプリケーションの使用を可能とする、前記通信網を介したアプリケーションとユーザ・インターフェースとの間の第 1 の接続と、

移動局と、

認証を可能にするように、移動局が登録されているデータ・ベースに接続可能なアプリケーションと、移動局との間の第 2 の通信網を介した第 2 の接続と、

第 2 の通信網を介して、アプリケーションに対するユーザを認証する手段とを含む配列。

【請求項 12】 移動局はセルラ電話であり、かつ移動通信網はデジタル通信網である請求項 11 記載の配列。

【請求項 13】 移動局へ及びからの認証シグナリングは、移動通信網の短メッセージ・システム（SMS）により与えられるテキスト・メッセージの形式にある請求項 11 又は 12 記載の配列。

【請求項 14】 移動局は、認証手順を制御するように配列された移動局の個人認証装置（MS PAD）と、秘密を含み、かつ MS PAD に作動的に接

続された加入者識別モジュール（SIM）と含み、SIMの秘密は、認証手順に利用されるように配列されている請求項11～13のいずれかに記載の配列。

【請求項15】 アプリケーションは、バンキング・サービス、電子ショッピング・サービス、又は電子トランザクションに対して肯定応答を必要とする他のいくつかの商業的サービスであることを特徴とする請求項11～14のうちのいずれかに記載の配列。

【請求項16】 通信網を通して提供されるアプリケーションに対して認証を与える移動局において、

アプリケーションは、通信網に接続されたユーザ・インターフェースによりアクセスされ、かつ

前記移動局は、通信のためにユーザ・インターフェース以外の異なる通信網を使用し、かつ移動局は、ユーザ・インターフェースによりアクセスされた前記アプリケーションの使用を認証するために使用される移動局。

【請求項17】 認証手順を制御するように配列された統合移動局の個人認証装置（MS PAD）を含む請求項16記載の移動局。

【請求項18】 局は、デジタル移動電話であり、かつ秘密を含む加入者識別モジュール（SIM）を含み、SIMの秘密は、認証手順に利用されるように配列されている請求項16又は17記載の移動局。

【請求項19】 少なくとも1つの追加的なSIMを含む請求項18記載の移動局。

【請求項20】 ユーザ・インターフェースと通信することが可能な赤外線又は無線トランシーバのようなユーザ・インターフェースと直接的にインターフェースをする手段を含む請求項16又は19記載の移動局。

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/EP 99/00763

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 G06F1/00 H04L29/06 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04Q G06F H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 668 876 A (FALK JOHAN PER ET AL) 16 September 1997	1,2,4, 11,12, 15,16,20 10
A	see column 3, line 21 - column 6, line 55 ---	
X	WO 95 19593 A (KEW MICHAEL JEREMY; LOVE JAMES SIMON (GB)) 20 July 1995	1,2,10, 11,16, 18,20 5,6,8,13
A	see page 7, line 10 - page 10, line 2 see page 13, line 29 - page 14, line 6 ---	
X	WO 96 13814 A (VAZVAN BEHRUZ) 9 May 1996	10
A	see page 3, line 7 - page 7, line 31 ---	1-6,8, 11-18
A	FR 2 740 291 A (SAGEM) 25 April 1997 see page 7, line 1 - line 32 -----	5,6,14, 15,19

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

15 June 1999

Date of mailing of the international search report

22/06/1999

Name and mailing address of the ISA

European Patent Office, P.B. 6518 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Behringer, L.V.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern: 1st Application No
PCT/EP 99/00763

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5668876 A	16-09-1997	AU 692881 B	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A	04-01-1996
		EP 0766902 A	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998
		WO 9600485 A	04-01-1996
WO 9519593 A	20-07-1995	AU 1390395 A	01-08-1995
		GB 2300288 A	30-10-1996
WO 9613814 A	09-05-1996	FI 945075 A	29-04-1996
		EP 0739526 A	30-10-1996
		FI 962553 A	25-11-1997
		FI 962961 A	28-08-1996
		FI 971009 A	26-04-1997
		FI 971248 A	26-04-1997
		FI 971848 A	30-04-1997
FR 2740291 A	25-04-1997	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(81)指定国 EP(AT, BE, CH, CY,
DE, DK, ES, FI, FR, GB, GR, IE, I
T, LU, MC, NL, PT, SE), OA(BF, BJ
, CF, CG, CI, CM, GA, GN, GW, ML,
MR, NE, SN, TD, TG), AP(GH, GM, K
E, LS, MW, SD, SZ, UG, ZW), EA(AM
, AZ, BY, KG, KZ, MD, RU, TJ, TM)
, AL, AM, AT, AU, AZ, BA, BB, BG,
BR, BY, CA, CH, CN, CU, CZ, DE, D
K, EE, ES, FI, GB, GD, GE, GH, GM
, HR, HU, ID, IL, IN, IS, JP, KE,
KG, KP, KR, KZ, LC, LK, LR, LS, L
T, LU, LV, MD, MG, MK, MN, MW, MX
, NO, NZ, PL, PT, RO, RU, SD, SE,
SG, SI, SK, SL, TJ, TM, TR, TT, U
A, UG, UZ, VN, YU, ZW